Extensions of local fields and truncated power series

Kevin Keating
Department of Mathematics
University of Florida
Gainesville, FL 32611
USA

keating@math.ufl.edu

Abstract

Let K be a finite tamely ramified extension of $\mathbb{Q}_p$ and let L/K be a totally ramified $(\mathbb{Z}/p^n\mathbb{Z})$-extension. Let π_L be a uniformizer for L, let σ be a generator for $\mathrm{Gal}(L/K)$, and let $f(X)$ be an element of $\emptyset_K[X]$ such that $\sigma(\pi_L) = f(\pi_L)$. We show that the reduction of $f(X)$ modulo the maximal ideal of $\emptyset_K$ determines a certain subextension of L/K up to isomorphism. We use this result to study the field extensions generated by periodic points of a p-adic dynamical system.

1 Introduction

Let p be a prime and let $\mathbb{Q}_p$ denote the p-adic numbers. In what follows all extensions of $\mathbb{Q}_p$ are contained in a fixed algebraic closure $\mathbb{Q}_p^{alg}$ of $\mathbb{Q}_p$. Let K be a finite extension of $\mathbb{Q}_p$ with ramification index e, let $\emptyset_K$ denote the ring of integers of K, and let $\mathcal{P}_K$ denote the maximal ideal of $\emptyset_K$. Let L/K be a totally ramified cyclic extension of degree p^n. Then the residue field $k = \emptyset_K/\mathcal{P}_K$ of K may be identified with a subring of $\emptyset_L/\mathcal{P}_L^{ep^n}$ using the Teichmüller lifting. Let σ be a generator for $\mathrm{Gal}(L/K)$ and let π_L be a uniformizer for L. Then there is a unique $h^{\sigma}_{\pi_L}(X) \in k[X]/(X^{ep^n})$ such that $\sigma(\pi_L) \equiv \pi_L h^{\sigma}_{\pi_L}(\pi_L) \pmod{\mathcal{P}_L^{ep^n+1}}$. The aim of this paper is to prove the following:

Theorem 1.1 *Let $p > 3$ and let K be a finite tamely ramified extension of $\mathbb{Q}_p$ with ramification index e. Let L/K and L'/K be totally ramified $(\mathbb{Z}/p^n\mathbb{Z})$-extensions such that L/K is contained in a $\mathbb{Z}_p$-extension L_∞/K. Assume:*

$$(*)\ \begin{cases} \text{There are generators } \sigma,\ \sigma' \text{ for } \mathrm{Gal}(L/K),\ \mathrm{Gal}(L'/K) \text{ and uniformizers} \\ \pi_L,\ \pi_{L'} \text{ for } L,\ L' \text{ such that } h^{\sigma}_{\pi_L} = h^{\sigma'}_{\pi_{L'}}. \end{cases}$$

Let m_0 be the largest integer such that $\psi_{L/K}((m_0 + 1 + \frac{1}{p-1})e) < ep^n$. Then there is $\omega \in \mathrm{Gal}(\mathbb{Q}_p^{alg}/\mathbb{Q}_p)$ such that $\omega(K) = K$, ω induces the identity on k, and $[L \cap \omega(L') : K] \geq p^{m_0}$.

The function $\psi_{L/K} : [-1, \infty) \to [-1, \infty)$ and its inverse $\phi_{L/K}$ are the Hasse-Herbrand functions of higher ramification theory. The basic properties of these functions can be found in Chapters IV and V of [8] for finite Galois extensions, and in the appendix of [2] for finite separable extensions. We will make frequent use of the formulas $\psi_{M/K} = \psi_{M/L} \circ \psi_{L/K}$ and $\phi_{M/K} = \phi_{L/K} \circ \phi_{M/L}$ for finite separable extensions $M \supset L \supset K$.

If K contains no primitive pth roots of unity then it can be shown using class field theory that L/K is contained in a $\mathbb{Z}_p$-extension (see Lemma 5.6). In any case, Theorem 1.1 is valid if either L/K or L'/K is contained in a $\mathbb{Z}_p$-extension. If neither of L/K, L'/K is contained in a $\mathbb{Z}_p$-extension, we still have the following result:

Theorem 1.2 *Let $p > 3$ and let K be a finite tamely ramified extension of $\mathbb{Q}_p$ with ramification index e. Let L/K and L'/K be totally ramified $\mathbb{Z}/p^n\mathbb{Z}$-extensions which satisfy (*). Then there is $\omega \in \mathrm{Gal}(\mathbb{Q}_p^{alg}/\mathbb{Q}_p)$ such that $\omega(K) = K$, ω induces the identity on k, and $[L \cap \omega(L') : K] \geq p^{m_0 - 1}$.*

Suppose $p > 3$ and $K/\mathbb{Q}_p$ is unramified. Then $m_0 = n - 1$ and K contains no primitive pth roots of unity. Furthermore, any automorphism of $\mathbb{Q}_p^{alg}$ which induces the identity on k also induces the identity on K and hence maps L onto itself. Therefore we get a simpler version of Theorem 1.1 in this case.

Corollary 1.3 *Let $p > 3$, let K be a finite unramified extension of $\mathbb{Q}_p$, and let L/K, L'/K be totally ramified $(\mathbb{Z}/p^n\mathbb{Z})$-extensions which satisfy (*). Then $[L \cap L' : K] \geq p^{n-1}$.*

Our proof of Theorem 1.1 is motivated by Wintenberger's proof of [9, Th. 2], but uses Deligne's theory of extensions of truncated valuation rings in place of the field of norms. In Section 2 we present a slightly modified version of Wintenberger's theorem and use it to prove a result which is related to Theorem 1.1. In Section 3 we give an outline of the theory of truncated local rings based on [2]. In Section 4 we prove a version of Theorem 1.1 for cyclotomic extensions. In Section 5 we use this special case to prove the theorem in general, and show how the same methods can be used to prove Theorem 1.2. In Section 6 we use a variant of Theorem 1.1 to study the field extensions generated by periodic points of a p-adic dynamical system.

2 The field of norms

In [10] and [9] Wintenberger describes a remarkable correspondence between groups of power series over fields of characteristic p and $\mathbb{Z}_p$-extensions of local fields. Theorem 1.1 may be viewed as a finite-level version of a part of this correspondence. In this section we describe the connection between Wintenberger's results and Theorem 1.1.

We begin by recalling the construction of the field of norms in a special case [11]. We define a local field to be a field complete with respect to a discrete valuation which has finite residue field. Let L_0 be a local field whose residue field k has characteristic p and let L_∞/L_0 be a totally ramified $\mathbb{Z}_p$-extension. For $n \geq 0$ let L_n/L_0 denote the subextension of L_∞/L_0 of degree p^n, let $\mathcal{O}_n$ denote the ring of integers of L_n, and let

$\mathcal{P}_n$ denote the maximal ideal of $\mathcal{O}_n$. Set $r_n = \lceil (p-1)i_n/p \rceil$, where i_n is the unique (upper and lower) ramification break of the $(\mathbb{Z}/p\mathbb{Z})$-extension L_{n+1}/L_n. It follows from [11, Prop. 2.2.1] that the norm N_{L_{n+1}/L_n} induces a ring homomorphism $\overline{\mathrm{N}}_{n+1,n}$ from $\mathcal{O}_{n+1}/(\mathcal{P}_{n+1}^{r_{n+1}})$ onto $\mathcal{O}_n/(\mathcal{P}_n^{r_n})$. The ring $A_{L_0}(L_\infty)$ is defined to be the inverse limit of the rings $\mathcal{O}_n/(\mathcal{P}_n^{r_n})$ with respect to the maps $\overline{\mathrm{N}}_{n+1,n}$. Since $\mathcal{O}_n/(\mathcal{P}_n^{r_n}) \cong k[X]/(X^{r_n})$ and $\lim_{n\to\infty} r_n = \infty$ we have $A_{L_0}(L_\infty) \cong k[[X]]$. The field of norms $X_{L_0}(L_\infty)$ of the extension L_∞/L_0 is defined to be the field of fractions of $A_{L_0}(L_\infty)$.

We define a compatible sequence of uniformizers for L_∞/L_0 to be a sequence $(\pi_n)_{n\geq 0}$ such that π_n is a uniformizer for L_n and $\mathrm{N}_{L_{n+1}/L_n}(\pi_{n+1}) = \pi_n$ for every $n \geq 0$. Associated to each compatible system of uniformizers for L_∞/L_0 we get a uniformizer $(\overline{\pi}_n)_{n\geq 0}$ for $X_{L_0}(L_\infty)$, where $\overline{\pi}_n$ denotes the image of π_n in $\mathcal{O}_n/\mathcal{P}_n^{r_n}$. By [11, Prop. 2.3.1] this construction gives a bijection between the set of compatible sequences of uniformizers for L_∞/L_0 and the set of uniformizers for $X_{L_0}(L_\infty)$.

Let $\sigma \in \mathrm{Gal}(L_\infty/L_0)$. Then for each $n \geq 0$ there is a unique $g_n(X) \in k[X]$ of degree $< r_n$ such that

$$\frac{\sigma\pi_n}{\pi_n} \equiv g_n(\pi_n) \pmod{\pi_n^{r_n}}, \tag{2.1}$$

where we identify k with a subring of $\mathcal{O}_n/\mathcal{P}_n^{r_n}$ using the Teichmüller lifting. If $n \geq 1$ we may apply $\overline{\mathrm{N}}_{n,n-1}$ to (2.1). Since $\overline{\mathrm{N}}_{n,n-1}$ is a ring homomorphism and $\mathrm{Gal}(L_n/L_0)$ is abelian we get

$$\frac{\sigma\pi_{n-1}}{\pi_{n-1}} \equiv g_n^\phi(\pi_{n-1}) \pmod{\pi_{n-1}^{r_{n-1}}}, \tag{2.2}$$

where $g_n^\phi(X)$ denotes the image of $g_n(X)$ under the automorphism of $k[X]$ induced by the p-Frobenius of k. It follows that

$$g_{n-1}(X) \equiv g_n^\phi(X) \pmod{X^{r_{n-1}}}. \tag{2.3}$$

Therefore there is $g_\sigma(X) \in k[[X]]$ such that

$$\frac{\sigma\pi_n}{\pi_n} \equiv g_\sigma^{\phi^{-n}}(\pi_n) \pmod{\pi_n^{r_n}} \tag{2.4}$$

for all $n \geq 0$. We define a k-linear action of $\mathrm{Gal}(L_\infty/L_0)$ on $X_{L_0}(L_\infty) \cong k(\!(X)\!)$ by setting $\sigma \cdot X = X g_\sigma(X)$.

Let $\mathcal{A}(k)$ denote the set of power series in $k[[X]]$ whose leading term has degree 1. Then $\mathcal{A}(k)$ with the operation of substitution forms a group. The map which carries $\sigma \in \mathrm{Aut}_k(k(\!(X)\!))$ onto $\sigma(X) \in \mathcal{A}(k)$ gives an isomorphism between $\mathrm{Aut}_k(k(\!(X)\!))$ and $\mathcal{A}(k)^{op}$. The subgroup $\mathcal{N}(k)$ of $\mathcal{A}(k)$ consisting of power series with leading term X is a pro-p group known as the Nottingham group [1]. Let $\Gamma_{L_\infty/L_0}^{(\pi_n)}$ denote the subgroup of $\mathcal{A}(k)$ consisting of power series of the form $Xg_\sigma(X)$ that arise from elements $\sigma \in \mathrm{Gal}(L_\infty/L_0)$ using the compatible sequence of uniformizers (π_n) for L_∞/L_0. Then $\Gamma_{L_\infty/L_0}^{(\pi_n)}$ is isomorphic to $\mathbb{Z}_p$. The subgroup $\Gamma_{L_\infty/L_0}^{(\pi_n)}$ of $\mathcal{A}(k)$ is determined up to conjugation by L_∞/L_0, and any subgroup of $\mathcal{A}(k)$ which is conjugate to $\Gamma_{L_\infty/L_0}^{(\pi_n)}$ is equal to $\Gamma_{L_\infty/L_0}^{(\tilde{\pi}_n)}$ for some compatible sequence of uniformizers $(\tilde{\pi}_n)$ for L_∞/L_0.

Let K, K' be local fields with residue field k and let L/K, L'/K' be totally ramified extensions. We say that L/K is k-isomorphic to L'/K' if there is an isomorphism $\tau : L \to L'$ such that $\tau(K) = K'$ and τ induces the identity on k. In this case we write $L/K \cong_k L'/K'$. Let $\mathcal{Z}(k)$ denote the set of k-isomorphism classes of totally ramified $\mathbb{Z}_p$-extensions L_∞/L_0 such that L_0 is a local field with residue field k. We put a metric on $\mathcal{Z}(k)$ by defining the distance between the classes $[L_\infty/L_0]$ and $[L'_\infty/L'_0]$ to be 2^{-m}, where $0 \leq m \leq \infty$ is the largest value such that $L_m/L_0 \cong_k L'_m/L'_0$, and $m = -1$ if L_0 is not k-isomorphic to L'_0. Let $\mathcal{G}(k)$ denote the set of conjugacy classes $[\Gamma]$ of subgroups of $\mathcal{A}(k)$ which are isomorphic to $\mathbb{Z}_p$. We put a metric on $\mathcal{G}(k)$ by defining the distance between $[\Gamma]$ and $[\Gamma']$ to be 2^{-m}, where m is the largest integer such that $h\Gamma h^{-1} \equiv \Gamma' \pmod{X^{m+1}}$ for some $h \in \mathcal{A}(k)$.

Since $\Gamma^{(\pi_n)}_{L_\infty/L_0}$ is determined up to conjugacy by the k-isomorphism class of L_∞/L_0, we denote its conjugacy class by $[\Gamma_{L_\infty/L_0}]$. The following result is essentially a special case of [3, Cor. 1.3].

Proposition 2.1 *The map $\Phi : \mathcal{Z}(k) \to \mathcal{G}(k)$ defined by $\Phi([L_\infty/L_0]) = [\Gamma_{L_\infty/L_0}]$ is a continuous bijection.*

Proof: Since $\lim_{n\to\infty} r_n = \infty$, the map Φ is continuous. To show that Φ is onto choose $[\Gamma] \in \mathcal{G}(k)$. By [9, Th. 1] there is a totally ramified $\mathbb{Z}_p$-extension L_∞/L_0 of local fields with residue field k and a field isomorphism $f : k(\!(X)\!) \to X_{L_0}(L_\infty)$ which induces an isomorphism between Γ and the subgroup of $\mathrm{Aut}(X_{L_0}(L_\infty))$ induced by $\mathrm{Gal}(L_\infty/L_0)$. We write

$$f : (k(\!(X)\!), \Gamma) \xrightarrow{\sim} (X_{L_0}(L_\infty), \mathrm{Gal}(L_\infty/L_0)). \tag{2.5}$$

Let ω be the automorphism of k induced by f and let Ω be an automorphism of the separable closure of L_∞ which induces ω on k. Let $L'_0 = \Omega^{-1}(L_0)$ and $L'_\infty = \Omega^{-1}(L_\infty)$. Then Ω^{-1} induces an isomorphism $\Upsilon : X_{L_0}(L_\infty) \to X_{L'_0}(L'_\infty)$, and

$$\Upsilon \circ f : (k(\!(X)\!), \Gamma) \longrightarrow (X_{L'_0}(L'_\infty), \mathrm{Gal}(L'_\infty/L'_0)) \tag{2.6}$$

is a k-linear isomorphism. It follows that $\Phi([L'_\infty/L'_0]) = [\Gamma]$.

To show that Φ is one-to-one suppose $[\Gamma_{L_\infty/L_0}] = [\Gamma_{L'_\infty/L'_0}]$. Then there are compatible sequences of uniformizers (π_n) for L_∞/L_0 and (π'_n) for L'_∞/L'_0 such that $\Gamma^{(\pi_n)}_{L_\infty/L_0} = \Gamma^{(\pi'_n)}_{L'_\infty/L'_0}$. Therefore there is an isomorphism

$$f : (X_{L_0}(L_\infty), \mathrm{Gal}(L_\infty/L_0)) \longrightarrow (X_{L'_0}(L'_\infty), \mathrm{Gal}(L'_\infty/L'_0)) \tag{2.7}$$

which maps $(\overline{\pi}_n)$ to $(\overline{\pi}'_n)$ and induces the identity on k. It follows from [9, Th. 2] that f is induced by a k-isomorphism from L_∞/L_0 to L'_∞/L'_0, and hence that $[L_\infty/L_0] = [L'_\infty/L'_0]$. □

We define the depth of $g(X) \in \mathcal{A}(k)$ to be the degree of the leading term of $(g(X) - X)/X$; the depth of $g(X) = X$ is taken to be ∞. Let Γ be a subgroup of $\mathcal{A}(k)$ which is isomorphic to $\mathbb{Z}_p$, and let γ be a generator for Γ. For $n \geq 0$ we define the

nth lower ramification break i_n of Γ to be the depth of γ^{p^n}; this definition is independent of the choice of γ. The upper ramification breaks of Γ are defined by the formulas $b_0 = i_0$ and $b_n - b_{n-1} = (i_n - i_{n-1})/p^n$ for $n \geq 1$. The b_n are integers by Sen's theorem [7]. It follows from [9, Cor. 3.3.4] that if $\Gamma = \Phi([L_\infty/L_0])$ then $(i_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ are the lower and upper ramification sequences of the $\mathbb{Z}_p$-extension L_∞/L_0. Note that since L_∞/L_0 is an arithmetically profinite extension [11, §1], the Hasse-Herbrand functions ϕ_{L_∞/L_0} and ψ_{L_∞/L_0} are defined, and the lower and upper ramification breaks of L_∞/L_0 are related by the formulas $b_n = \phi_{L_\infty/L_0}(i_n)$ and $i_n = \psi_{L_\infty/L_0}(b_n)$ for $n \geq 0$. For future use we recall the following facts about the upper ramification breaks of a cyclic extension (see for instance [6, p. 280]).

Lemma 2.2 *Let K be a local field with residue characteristic p and let L/K be a totally ramified $(\mathbb{Z}/p^n\mathbb{Z})$-extension. Let $1 \leq e \leq \infty$ be the K-valuation of p and let $b_0 < b_1 < \cdots < b_{n-1}$ be the upper ramification breaks of L/K. Then for $0 \leq i \leq n-2$ we have:*

(a) $1 \leq b_0 \leq pe/(p-1)$;

(b) If $b_i \leq e/(p-1)$ *then* $pb_i \leq b_{i+1} \leq pe/(p-1)$;

(c) If $b_i \geq e/(p-1)$ *then* $b_{i+1} = b_i + e$.

Let $\mathcal{Z}_0(k)$ denote the subspace of $\mathcal{Z}(k)$ consisting of k-isomorphism classes of $\mathbb{Z}_p$-extensions in characteristic 0 and let $\mathcal{G}_0(k) = \Phi(\mathcal{Z}_0(k))$.

Corollary 2.3 $\Phi|_{\mathcal{Z}_0(k)} : \mathcal{Z}_0(k) \to \mathcal{G}_0(k)$ *is a homeomorphism.*

Proof: For $1 \leq e < \infty$ let $\mathcal{Z}_0^e(k)$ denote the subspace of $\mathcal{Z}_0(k)$ consisting of k-isomorphism classes of $\mathbb{Z}_p$-extensions $[L_\infty/L_0]$ such that the absolute ramification index of L_0 is e, and let $\mathcal{G}_0^e(k) = \Phi(\mathcal{Z}_0^e(k))$. Then $\mathcal{Z}_0^e(k)$ is open in $\mathcal{Z}(k)$. It follows from Krasner's Lemma that there are only finitely many isomorphism classes of local fields L_0 with residue field k and absolute ramification index e. For each such L_0 consider the set $\mathcal{H}_{L_0}$ of continuous homomorphisms $\chi : L_0^\times \to \mathbb{Z}_p$ such that $\chi(\mathcal{O}_{L_0}^\times) = \mathbb{Z}_p$. This set is compact, and class field theory gives a continuous map from $\mathcal{H}_{L_0}$ onto the set of all elements of $\mathcal{Z}_0^e(k)$ of the form $[L_\infty/L_0]$. Therefore $\mathcal{Z}_0^e(k)$ is compact. Since Φ is a continuous bijection, it follows that

$$\Phi|_{\mathcal{Z}_0^e(k)} : \mathcal{Z}_0^e(k) \longrightarrow \mathcal{G}_0^e(k) \tag{2.8}$$

is a homeomorphism.

Let $[\Gamma] \in \mathcal{G}_0^e(k)$ and let $[L_\infty/L_0] \in \mathcal{Z}_0^e(k)$ be such that $\Phi([L_\infty/L_0]) = [\Gamma]$. Let $(b_n)_{n\geq 0}$ be the upper ramification sequence of L_∞/L_0 and Γ. It follows from Lemma 2.2 that there is $M \geq 1$ such that $b_n - b_{n-1} = e$ for all $n \geq M$. If $[\Gamma'] \in \mathcal{G}_0(k)$ is sufficiently close to $[\Gamma]$ then the first $M+2$ upper ramification breaks $b'_0, b'_1, \ldots, b'_{M+1}$ of Γ' are the same as those of Γ. In particular, we have $b'_M - b'_{M-1} = b'_{M+1} - b'_M = e$. Let $[L'_\infty/L'_0]$ be the unique element of $\mathcal{Z}_0(k)$ such that $\Phi([L'_\infty/L'_0]) = [\Gamma']$. Then the upper ramification breaks of L'_∞/L'_0 are the same as those of Γ', so by Lemma 2.2 the absolute ramification

index of L_0' is e. It follows that $[\Gamma'] \in \mathcal{G}_0^e(k)$, and hence that $\mathcal{G}_0^e(k)$ is open in $\mathcal{G}_0(k)$. Since (2.8) is a homeomorphism for $1 \leq e < \infty$, we conclude that Φ induces a homeomorphism between $\mathcal{Z}_0(k)$ and $\mathcal{G}_0(k)$. $\square$

Let $\mathcal{Z}_p(k)$ denote the subspace of $\mathcal{Z}(k)$ consisting of k-isomorphism classes of $\mathbb{Z}_p$-extensions in characteristic p and let $\mathcal{G}_p(k) = \Phi(\mathcal{Z}_p(k))$. Using [9, 3.3] and Krasner's Lemma one can show that Φ induces a homeomorphism between $\mathcal{Z}_p(k)$ and $\mathcal{G}_p(k)$. But Φ itself is not a homeomorphism. Indeed, if $[L_\infty/L_0] \in \mathcal{Z}_p(k)$ then by the methods of the next section one can construct $[L'_\infty/L'_0] \in \mathcal{Z}_0(k)$ such that $\Phi([L'_\infty/L'_0])$ is arbitrarily close to $\Phi([L_\infty/L_0])$. Since the distance between $[L_\infty/L_0]$ and $[L'_\infty/L'_0]$ is always 2, this implies that Φ is not a homeomorphism.

Since $\mathcal{G}_0^e(k)$ is compact, it follows from Corollary 2.3 that the map

$$\Phi^{-1}|_{\mathcal{G}_0^e(k)} : \mathcal{G}_0^e(k) \longrightarrow \mathcal{Z}_0^e(k) \tag{2.9}$$

is uniformly continuous. From this fact we deduce the following non-effective version of Theorem 1.1:

Corollary 2.4 *Let $e \geq 1$ and let k be a finite field of characteristic p. Then there is a nondecreasing function $s : \mathbb{N} \to \mathbb{N} \cup \{0\}$ such that $\lim_{n\to\infty} s(n) = \infty$ which has the following property: Let L_0, L_0' be finite extensions of $\mathbb{Q}_p$ with residue field k and absolute ramification index e, and let L_∞/L_0 and L'_∞/L'_0 be totally ramified $\mathbb{Z}_p$-extensions such that*

$$\Gamma^{(\pi_n)}_{L_\infty/L_0} \equiv \Gamma^{(\pi'_n)}_{L'_\infty/L'_0} \pmod{X^{m+1}} \tag{2.10}$$

for some $m \geq 1$ and some compatible sequences of uniformizers (π_n) for L_∞/L_0 and (π'_n) for L'_∞/L'_0. Then $L_{s(m)}/L_0 \cong_k L'_{s(m)}/L'_0$.

3 Truncated valuation rings

In this section we give an overview of Deligne's theory of extensions of truncated valuation rings. For more details see [2].

Define a category $\mathcal{T}$ whose objects are triples (A, M, ϵ) such that:

1. A is an Artin local ring whose maximal ideal m_A is principal and whose residue field is finite.

2. M is a free A-module of rank 1.

3. $\epsilon : M \to A$ is an A-module homomorphism whose image is m_A.

Let $S_1 = (A_1, M_1, \epsilon_1)$ and $S_2 = (A_2, M_2, \epsilon_2)$ be elements of $\mathcal{T}$. A morphism from S_1 to S_2 is a triple $f = (r, \mu, \eta)$, where r is a positive integer, $\mu : A_1 \to A_2$ is a ring homomorphism, and $\eta : M_1 \to M_2^{\otimes r}$ is an A_1-module homomorphism. These must satisfy $\mu \circ \epsilon_1 = \epsilon_2^{\otimes r} \circ \eta$, and the map $M_1 \otimes_{A_1} A_2 \to M_2^{\otimes r}$ induced by η must be an isomorphism of A_2-modules. Let $S_3 = (A_3, M_3, \epsilon_3)$ be another element of $\mathcal{T}$, and let

$g = (s, \nu, \theta) : S_2 \to S_3$ be a morphism. Then the composition of g with f is defined to be $g \circ f = (sr, \nu \circ \mu, \theta^{\otimes r} \circ \eta)$. Thus the identity morphism on S_1 is $(1, \mathrm{id}_{A_1}, \mathrm{id}_{M_1})$, and f is an isomorphism if and only if $r = 1$, μ is an isomorphism, and η is an isomorphism. Let $f = (r, \mu, \eta)$ and $f' = (r', \mu', \eta')$ be morphisms from S_1 to S_2, and let c be a positive integer. We say f and f' are $R(c)$-equivalent, or $f \equiv f' \pmod{R(c)}$, if $r = r'$, μ and μ' induce the same map on residue fields, and $\eta(x) - \eta'(x) \in m_{A_2}^{rc} M_2^{\otimes r}$ for all $x \in M_1$.

Let $f = (r, \mu, \eta) : S_1 \to S_2$ be a $\mathcal{T}$-morphism. We say that (S_2, f) is an extension of S_1 if $\mathrm{length}(A_2) = r \cdot \mathrm{length}(A_1)$. We will often denote the extension (S_2, f) by S_2/S_1. Let (S_2, f) and (S_3, g) be extensions of S_1. A morphism from (S_2, f) to (S_3, g) is defined to be a $\mathcal{T}$-morphism $h : S_2 \to S_3$ such that $h \circ f = g$. If (S_2', f') is an extension of S_1', we say that S_2'/S_1' is isomorphic to S_2/S_1 if there are isomorphisms $i : S_1' \to S_1$ and $j : S_2' \to S_2$ such that $j \circ f' = f \circ i$.

Let K be a local field and let e be a positive integer. Define the e-truncation $\mathrm{Tr}_e(K)$ of K to be the triple (A, M, ϵ) consisting of the ring $A = \emptyset_K/\mathcal{P}_K^e$, the A-module $M = \mathcal{P}_K/\mathcal{P}_K^{e+1}$, and the A-module homomorphism $\epsilon : M \to A$ induced by the inclusion $\mathcal{P}_K \hookrightarrow \emptyset_K$. It is clear that $\mathrm{Tr}_e(K)$ is an element of $\mathcal{T}$. Conversely, every element of $\mathcal{T}$ is isomorphic to $\mathrm{Tr}_e(K)$ for some finite extension K of $\mathbb{Q}_p$ and some $e \geq 1$ (cf. [2, 1.2]).

Let K and L be local fields, let $\sigma : K \to L$ be an embedding, and let r be the ramification index of L over $\sigma(K)$. Define a morphism

$$f_\sigma = (r, \mu_\sigma, \eta_\sigma) : \mathrm{Tr}_e(K) \longrightarrow \mathrm{Tr}_{re}(L) \tag{3.1}$$

where

$$\mu_\sigma : \emptyset_K/\mathcal{P}_K^e \longrightarrow \emptyset_L/\mathcal{P}_L^{re} \tag{3.2}$$

$$\eta_\sigma : \mathcal{P}_K/\mathcal{P}_K^{e+1} \longrightarrow \mathcal{P}_L^r/\mathcal{P}_L^{re+r} \cong (\mathcal{P}_L/\mathcal{P}_L^{re+1})^{\otimes r} \tag{3.3}$$

are induced by σ. Then $(\mathrm{Tr}_{re}(L), f_\sigma)$ is an extension of $\mathrm{Tr}_e(K)$. If L is a finite extension of K with ramification index r we write $f_{L/K} = (r, \mu_{L/K}, \eta_{L/K})$ for the morphism from $\mathrm{Tr}_e(K)$ to $\mathrm{Tr}_{re}(L)$ induced by the inclusion $K \hookrightarrow L$. The following proposition shows that all extensions of $\mathrm{Tr}_e(K)$ are produced by this construction.

Proposition 3.1 *([2, Lemme 1.4.4]) Let K be a local field, let $e \geq 1$, and let (T, f) be an extension of $\mathrm{Tr}_e(K)$, with $f = (r, \mu, \eta)$. Then there is a finite extension L/K such that $(T, f) \cong (\mathrm{Tr}_{re}(L), f_{L/K})$.*

Let $d \geq 0$ be real, let L/K be a finite extension of local fields, and let N/K be the normal closure of L/K in L^{sep}. We denote the largest upper ramification break of L/K by $u_{L/K}$. We say that L/K satisfies condition C^d if $d > u_{L/K}$, or equivalently, if the ramification subgroup $\mathrm{Gal}(N/K)^d$ is trivial. Let $\mathrm{ext}(K)^d$ denote the category whose objects are finite extensions of K which satisfy condition C^d, and whose morphisms are K-inclusions.

Let $S \in \mathcal{T}$ and let (T, f) be an extension of S. Then there are positive integers r, e and a finite extension of local fields L/K such that $T/S \cong \mathrm{Tr}_{re}(L)/\mathrm{Tr}_e(K)$. Given $0 \leq d \leq e$ we say that T/S satisfies condition C^d if L/K satisfies condition C^d. This

definition is independent of the choice of L/K. One can associate ramification data to the extension T/S. In particular, the Hasse-Herbrand functions $\phi_{T/S}$ and $\psi_{T/S}$ are defined. It follows from [2, 1.5.3] that if T/S satisfies condition C^e then $\phi_{T/S} = \phi_{L/K}$ and $\psi_{T/S} = \psi_{L/K}$.

Let $S \in \mathcal{T}$. We define a category $\mathrm{ext}(S)^d$ whose objects are extensions of S which satisfy condition C^d. An $\mathrm{ext}(S)^d$-morphism from (T_1, f_1) to (T_2, f_2) is defined to be an $R(\psi_{T_1/S}(d))$-equivalence class of morphisms from (T_1, f_1) to (T_2, f_2). The main result of [2] is the following.

Theorem 3.2 *([2, Théorème 2.8]) Let K be a local field and let e be a positive integer. Then the functor from $\mathrm{ext}(K)^e$ to $\mathrm{ext}(\mathrm{Tr}_e(K))^e$ which maps L/K to $\mathrm{Tr}_{re}(L)/\mathrm{Tr}_e(K)$ is an equivalence of categories.*

The proof of Theorem 1.1 depends on the following application of Theorem 3.2:

Corollary 3.3 *Let e be a positive integer and let L/K and L'/K be finite extensions of local fields which have ramification index r and satisfy condition C^e. Let $\tau \in \mathrm{Aut}(K)$ and let $j : \mathrm{Tr}_{re}(L') \to \mathrm{Tr}_{re}(L)$ be an isomorphism such that $j \circ f_{L'/K} = f_{L/K} \circ f_\tau$. Then there is a unique isomorphism $\gamma : L' \to L$ such that $j \equiv f_\gamma \pmod{R(\psi_{L/K}(e))}$ and $\gamma|_K = \tau$.*

Proof: Let $i : K \hookrightarrow L$ and $i' : K \hookrightarrow L'$ be the inclusion maps. Then $(\mathrm{Tr}_{re}(L'), f_{L'/K})$ and $(\mathrm{Tr}_{re}(L), f_{L/K} \circ f_\tau)$ are elements of $\mathrm{ext}(\mathrm{Tr}_e(K))^e$ which are induced by i' and $i \circ \tau$. Since j gives an isomorphism between these extensions, by Theorem 3.2 there is a unique isomorphism $\gamma : L' \to L$ such that $j \equiv f_\gamma \pmod{R(\psi_{L/K}(e))}$ and $\gamma \circ i' = i \circ \tau$. □

4 Recognizing cyclotomic extensions

Before proving Theorem 1.1 we prove the following result, which may be viewed as a special case of the theorem. An analogous result in the setting of the field of norms is proved in [9, Prop. 3].

Proposition 4.1 *Let $p > 2$ and let $F/\mathbb{Q}_p$ be a finite tamely ramified extension with ramification index e. Set $s = (p-1)/\gcd(e, p-1)$ and $e_0 = e/\gcd(e, p-1)$. Let $m \geq 1$, let E/F be a totally ramified cyclic extension of degree sp^m, and let d be an integer such that $p \nmid d$ and the image of d in $(\mathbb{Z}/p^{m+1}\mathbb{Z})^\times$ has order sp^m. Assume there is $\alpha \in E$ such that $v_E(\alpha - 1) = e_0$ and a generator τ for $\mathrm{Gal}(E/F)$ such that $\tau(\alpha) \equiv \alpha^d \pmod{\mathcal{P}_E^n}$ for some $n > e_0 p^m$. Then there is a primitive p^{m+1}th root of unity $\xi \in \mathbb{Q}_p^{alg}$ such that $v_E(\alpha - \xi) \geq (gs + e_0)p^m$, where*

$$g = \left\lceil \frac{n - e_0(p^{m+1} + p^m - 1)}{sp^m} \right\rceil. \tag{4.1}$$

In particular, if $n > e_0(p^{m+1} + p^m - 1)$ then $E = F(\xi)$.

For $t \in \mathbb{Z}$ let $f(t)$ denote the maximum value of $v_E(\tau(\beta)\beta^{-1} - d)$ as β ranges over the compact set $C_t = \{\beta \in E : v_E(\beta) = t\}$. Since $\mathrm{N}_{E/F}(d) \neq 1$ we have $\tau(\beta)\beta^{-1} \neq d$ for all $\beta \in C_t$, so $f(t) \in \mathbb{Z}$. The proof of Proposition 4.1 depends on the following lemma:

Lemma 4.2 *Let $t \in \mathbb{Z}$ and set $t_0 = t - e_0 p^m$. Then*

$$f(t) = \begin{cases} 0 & \text{if } s \nmid t_0, \\ e_0(p^{v_p(t_0)+1} - 1) & \text{if } s \mid t_0 \text{ and } v_p(t_0) < m, \\ e_0(p^{m+1} - 1) & \text{if } s \mid t_0 \text{ and } v_p(t_0) \geq m. \end{cases} \tag{4.2}$$

The proof of Lemma 4.2 uses the following result, which follows easily from Proposition 8 in [8, V].

Proposition 4.3 *Let E be a local field and let M/E be a finite totally ramified Galois extension. Let d be a positive integer and let x, y be elements of $\emptyset_M^\times$ such that $x \equiv y \pmod{\mathcal{P}_M^{\psi_{M/E}(d)+1}}$. Then $\mathrm{N}_{M/E}(x) \equiv \mathrm{N}_{M/E}(y) \pmod{\mathcal{P}_E^{d+1}}$.*

Proof of Lemma 4.2: Since E/F is totally ramified and $p \nmid e_0$ we can write $\alpha = 1 + c\pi_E^{e_0}$, where $c \in \emptyset_F^\times$ and π_E is a uniformizer for E. Since $v_p(d^s - 1) = 1$ and $v_E(\alpha^p - 1) = pe_0$, we have $v_E(\tau^s(\alpha) - \alpha) = pe_0$. It follows that $v_E(\tau^s(\pi_E^{e_0}) - \pi_E^{e_0}) = pe_0$, and hence that $v_E(\tau^s(\pi_E^{e_0})\pi_E^{-e_0} - 1) = (p-1)e_0$. Since τ^s has order p^m we have $v_E(\tau^s(\pi_E)\pi_E^{-1} - 1) \geq 1$, and hence $v_E(\tau^s(\pi_E)\pi_E^{-1} - 1) = (p-1)e_0$. Let T/F denote the maximum tamely ramified subextension of E/F. Then T is the subfield of E fixed by $\langle \tau^s \rangle$, so the smallest (upper and lower) ramification break of E/T is $(p-1)e_0$. Since $(p-1)e_0 = v_T(p)$, by Lemma 2.2(c) we deduce that for $0 \leq i < m$ the ith upper ramification break of E/T is $(p-1)e_0(i+1)$. It follows that the ith lower ramification break of E/T is $\psi_{E/T}((p-1)e_0(i+1)) = e_0(p^{i+1} - 1)$.

Let $\gamma = \alpha - 1 = c\pi_E^{e_0}$. Then

$$\frac{\tau(\gamma)}{\gamma} \equiv \frac{(1+\gamma)^d - 1}{\gamma} \equiv d \pmod{\mathcal{P}_E^{e_0}}. \tag{4.3}$$

Since the smallest upper ramification break of E/T is $(p-1)e_0$, we have $\psi_{E/T}(e_0 - 1) = e_0 - 1$. Applying Proposition 4.3 to (4.3) we get

$$\mathrm{N}_{E/T}\left(\frac{\tau(\gamma)}{\gamma}\right) \equiv \mathrm{N}_{E/T}(d) \pmod{\mathcal{P}_T^{e_0}}. \tag{4.4}$$

Let $\delta = \mathrm{N}_{E/T}(\gamma)$. Since $\mathrm{Gal}(E/F)$ is commutative, (4.4) reduces to

$$\frac{\tau(\delta)}{\delta} \equiv d^{p^m} \equiv d \pmod{\mathcal{P}_T^{e_0}}. \tag{4.5}$$

Since both sides of (4.2) depend only on the congruence class of t modulo sp^m, we may assume $e_0 p^m \leq t < (e_0 + s)p^m$. Let β be an element of E such that $v_E(\beta) = t$, and

set $\kappa = \beta\delta^{-1}$. Then by (4.5) we have

$$\frac{\tau(\beta)}{\beta} - d = \frac{\tau(\kappa)}{\kappa} \cdot \frac{\tau(\delta)}{\delta} - d \tag{4.6}$$

$$\equiv \left(\frac{\tau(\kappa)}{\kappa} - 1\right) d \pmod{\mathcal{P}_E^{e_0 p^m}}. \tag{4.7}$$

For $0 < t_0 < sp^m$ let $g(t_0)$ denote the maximum value of $v_E(\tau(\kappa)\kappa^{-1} - 1)$ as κ ranges over C_{t_0}. It follows from Sen's argument in [7, p. 35] that $g(t_0)$ is equal to the ramification number $v_E(\tau^{t_0}(\pi_E)\pi_E^{-1} - 1)$ of τ^{t_0}. Thus if $s \nmid t_0$ then $g(t_0) = 0$, while if $s \mid t_0$ and $v_p(t_0) = i$ then $g(t_0) = e_0(p^{i+1} - 1)$ is the ith lower ramification break of E/T. It follows that $g(t_0) < e_0 p^m$ for $0 < t_0 < sp^m$. Hence by (4.7) we get $g(t_0) = f(t_0 + e_0 p^m)$. This proves the lemma for all t such that $e_0 p^m < t < (e_0 + s)p^m$.

It remains to prove the lemma for $t = e_0 p^m$. For $e_0 p^m \le t < (e_0 + s)p^m$ let β_t be an element of E such that $v_E(\beta_t) = t$ and $v_E((\tau - d)\beta_t)$ is maximized. Let Λ denote the $\mathcal{O}_F$-lattice spanned by the β_t. Then $\Lambda = \pi_E^{e_0 p^m}\mathcal{O}_E$ is an ideal in $\mathcal{O}_E$, and hence $(\tau - d)\Lambda$ is contained in Λ. It follows from the maximality of $v_E((\tau - d)\beta_t)$ that the integers $v_E((\tau - d)\beta_t)$ for $e_0 p^m \le t < (e_0 + s)p^m$ represent distinct congruence classes modulo sp^m. Therefore $\Lambda/(\tau - d)\Lambda$ is an $\mathcal{O}_F$-module of length

$$\sum_{t=e_0 p^m}^{(e_0+s)p^m - 1} v_E((\tau - d)\beta_t) \;-\; \sum_{t=e_0 p^m}^{(e_0+s)p^m - 1} v_E(\beta_t) = \sum_{t=e_0 p^m}^{(e_0+s)p^m - 1} f(t). \tag{4.8}$$

It follows that

$$\sum_{t=e_0 p^m}^{(e_0+s)p^m - 1} f(t) = v_E(\det(\tau - d)). \tag{4.9}$$

Since the characteristic polynomial of the F-linear map $\tau : E \to E$ is $h(X) = X^{sp^m} - 1$, the determinant of $\tau - d$ is $\pm h(d) = \pm(d^{sp^m} - 1)$. Therefore we have

$$\sum_{t=e_0 p^m}^{(e_0+s)p^m - 1} f(t) = v_E(d^{sp^m} - 1) \tag{4.10}$$

$$= (m + 1)e_0(p^{m+1} - p^m). \tag{4.11}$$

Solving for $f(e_0 p^m)$ in terms of the known values of $f(t)$ gives $f(e_0 p^m) = e_0(p^{m+1} - 1)$, which completes the proof of the lemma. □

Proof of Proposition 4.1: It follows from the hypotheses that $v_E(\alpha^{p^{m+1}} - 1) \ge e_0 p^{m+1}$, and that

$$v_E(\tau(\alpha^{p^{m+1}}) - \alpha^{dp^{m+1}}) \ge n + (m + 1)e_0(p^{m+1} - p^m). \tag{4.12}$$

Let $\lambda = \log(\alpha^{p^{m+1}})$. Then we have

$$v_E(\tau(\lambda) - d\lambda) = v_E(\tau(\alpha^{p^{m+1}}) - \alpha^{dp^{m+1}}), \tag{4.13}$$

and hence

$$v_E(\lambda) + v_E\left(\frac{\tau(\lambda)}{\lambda} - d\right) \geq n + (m+1)e_0(p^{m+1} - p^m). \tag{4.14}$$

Set $t = v_E(\lambda) = v_E(\alpha^{p^{m+1}} - 1)$. Then by (4.14) we get

$$t + f(t) \geq n + (m+1)e_0(p^{m+1} - p^m), \tag{4.15}$$

where $f(t)$ is the function defined in Lemma 4.2.

If $f(t) > 0$ then by Lemma 4.2 we have $t = e_0p^m + csp^i$ and $f(t) = e_0(p^{i+1} - 1)$ for some $0 \leq i \leq m$ and $c \in \mathbb{Z}$. It follows from (4.15) that

$$e_0p^m + csp^i + e_0(p^{i+1} - 1) \geq n + (m+1)e_0(p^{m+1} - p^m), \tag{4.16}$$

which implies

$$csp^i \geq e_0(p^{m+1} - p^{i+1}) + (m+1)e_0(p^{m+1} - p^m) + n - e_0(p^{m+1} + p^m - 1). \tag{4.17}$$

Dividing by sp^i and using the fact that s divides $p-1$ we get

$$c \geq e_0\frac{p^{m+1} - p^{i+1}}{sp^i} + (m+1)e_0\frac{p^{m+1} - p^m}{sp^i} + \left\lceil \frac{n - e_0(p^{m+1} + p^m - 1)}{sp^i} \right\rceil. \tag{4.18}$$

It follows that

$$t \geq e_0p^m + e_0(p^{m+1} - p^{i+1}) + (m+1)e_0(p^{m+1} - p^m) + sp^i \left\lceil \frac{n - e_0(p^{m+1} + p^m - 1)}{sp^i} \right\rceil. \tag{4.19}$$

The minimum value of right hand side of (4.19) for $0 \leq i \leq m$ is achieved when $i = m$. Therefore the inequality

$$t \geq e_0p^m + (m+1)e_0(p^{m+1} - p^m) + sp^m \left\lceil \frac{n - e_0(p^{m+1} + p^m - 1)}{sp^m} \right\rceil \tag{4.20}$$

holds for all t such that $f(t) > 0$. If $f(t) = 0$ then by (4.15) we have

$$t \geq n + (m+1)e_0(p^{m+1} - p^m), \tag{4.21}$$

which implies that (4.20) holds in this case as well. Thus (4.20) is valid in general.

Let $\zeta \in \mathbb{Q}_p^{alg}$ be a primitive p^{m+1}th root of unity, and choose $0 \leq j < p^{m+1}$ to maximize $w = v_E(\alpha - \zeta^j)$. For $0 \leq i < p^{m+1}$ we have

$$v_E(\alpha - \zeta^i) \geq \min\{w, v_E(\zeta^j - \zeta^i)\}, \tag{4.22}$$

with equality if $w > v_E(\zeta^j - \zeta^i)$. Since $w \geq v_E(\alpha - \zeta^i)$, this implies that for $i \neq j$ we have $v_E(\alpha - \zeta^i) \leq v_E(\zeta^j - \zeta^i) = e_0p^{v_p(i-j)}$. Since

$$\alpha^{p^{m+1}} - 1 = (\alpha - 1)(\alpha - \zeta)(\alpha - \zeta^2)\dots(\alpha - \zeta^{p^{m+1}-1}), \tag{4.23}$$

by defining $p^{v_p(0)} = 0$ we get

$$t = v_E(\alpha^{p^{m+1}} - 1) \le w + \sum_{i=0}^{p^{m+1}-1} e_0 p^{v_p(i-j)} \tag{4.24}$$

$$= w + (m+1)e_0(p^{m+1} - p^m). \tag{4.25}$$

By comparing (4.20) with (4.25) we conclude that $w \ge gsp^m + e_0p^m$, where g is the integer defined in (4.1). Set $\xi = \zeta^j$; then $v_E(\alpha - \xi) = w \ge gsp^m + e_0p^m$. Since $v_E(\alpha - \xi) > e_0$, we have $v_E(\xi - 1) = v_E(\alpha - 1) = e_0$, so ξ is a primitive p^{m+1}th root of unity. If $n > e_0(p^{m+1} + p^m - 1)$ then $g \ge 1$, and hence $v_E(\alpha - \xi) > e_0p^m$. Therefore by Krasner's Lemma we have $F(\alpha) \supset F(\xi)$. Since $E \supset F(\alpha)$ and $[F(\xi) : F] \ge sp^m = [E : F]$, this implies $E = F(\xi)$. □

5 Proof of Theorem 1.1

In this section we prove Theorem 1.1 in a somewhat generalized form. Let $1 \le a \le ep^n$ and $1 \le m \le n$. We will show that $[\omega(L) \cap L' : K] \ge p^m$ whenever

$$h^{\sigma}_{\pi_L}(X) \equiv h^{\sigma'}_{\pi_{L'}}(X) \pmod{X^a} \tag{5.1}$$

and a and m satisfy certain inequalities, which are specified in Theorem 5.2. We then show in Lemmas 5.7 and 5.8 that the values $a = ep^n$ and $m = m_0$ given in Theorem 1.1 satisfy these inequalities. To motivate the proof we first prove an analog of Theorem 1.1 for local fields of characteristic p.

Proposition 5.1 *Let K be a local field of characteristic p with residue field k and let L/K, L'/K be totally ramified $(\mathbb{Z}/p^n\mathbb{Z})$-extensions. Let $u_{L/K}$ be the largest upper ramification break of L/K, let $e > u_{L/K}$, and let $h(X) \in k[X]$. Assume there exist uniformizers $\pi_L, \pi_{L'}$ for L, L' and generators σ, σ' for $\mathrm{Gal}(L/K)$, $\mathrm{Gal}(L'/K)$ such that*

$$\sigma(\pi_L) \equiv \pi_L h(\pi_L) \pmod{\mathcal{P}_L^{ep^n+1}} \tag{5.2}$$

$$\sigma'(\pi_{L'}) \equiv \pi_{L'} h(\pi_{L'}) \pmod{\mathcal{P}_{L'}^{ep^n+1}}. \tag{5.3}$$

Then the extensions L/K and L'/K are k-isomorphic.

Proof: Let $\alpha : L' \to L$ be the unique k-isomorphism such that $\alpha(\pi_{L'}) = \pi_L$. Since $\pi_K = \mathrm{N}_{L/K}(\pi_L)$ and $\pi'_K = \mathrm{N}_{L'/K}(\pi_{L'})$ are uniformizers for K there is a unique k-automorphism τ of K such that $\tau(\pi'_K) = \pi_K$. It follows from (5.2) and (5.3) that

$$\tau(\pi'_K) \equiv \alpha(\pi'_K) \pmod{\mathcal{P}_L^{ep^n+1}}. \tag{5.4}$$

Therefore the induced maps

$$f_{L/K} : \mathrm{Tr}_e(K) \longrightarrow \mathrm{Tr}_{ep^n}(L) \tag{5.5}$$

$$f_{L'/K} : \mathrm{Tr}_e(K) \longrightarrow \mathrm{Tr}_{ep^n}(L') \tag{5.6}$$

$$f_{\tau} : \mathrm{Tr}_e(K) \longrightarrow \mathrm{Tr}_e(K) \tag{5.7}$$

$$f_{\alpha} : \mathrm{Tr}_{ep^n}(L') \longrightarrow \mathrm{Tr}_{ep^n}(L) \tag{5.8}$$

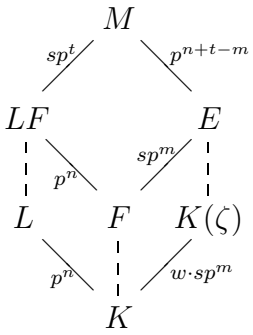

Figure 1: Dashed lines represent unramified extensions.

satisfy $f_\alpha \circ f_{L'/K} = f_{L/K} \circ f_\tau$. Since $u_{L/K} = u_{L'/K} < e$, both L/K and L'/K satisfy condition C^e. Therefore by Corollary 3.3 there is a k-isomorphism $\gamma : L' \to L$ such that $\gamma|_K = \tau$. Hence $L'/K \cong_k L/K$. □

To apply this method in characteristic 0 we replace the fields K, L, L' with cyclotomic extensions. This makes our fields resemble local fields of characteristic p and allows us to replace (5.1) with a congruence modulo a higher power of X. Let $\zeta \in \mathbb{Q}_p^{alg}$ be a primitive p^{m+1}th root of unity and set $M = L(\zeta)$. Then M/K is an abelian extension whose Galois group may be identified with a subgroup of $\mathrm{Gal}(L/K) \times \mathrm{Gal}(K(\zeta)/K)$. We will use the theory of truncated local rings outlined in Section 3 to define an extension M'/L' which corresponds to M/L. We will then use Proposition 4.1 to show that in fact $M' = L'(\zeta)$. Let L_0/K, L_0'/K be the subextensions of L/K, L'/K of degree p^m. Using Corollary 3.3 we will show that $L_0(\zeta)/K \cong_k L_0'(\zeta)/K$, from which it will follow that $L_0/K \cong_k L_0'/K$.

Let w denote the residue class degree and sp^m the ramification index of $K(\zeta)/K$. Then the ramification index of M/L is equal to sp^t for some $0 \le t \le m$. Let F/K be the maximum unramified subextension of M/K and let $E/K(\zeta)$ be the maximum unramified subextension of $M/K(\zeta)$. Then E/F is a totally ramified cyclic extension of degree sp^m, and M/E is a totally ramified cyclic extension of degree p^{n+t-m} (see Figure 1).

In order to state our generalized version of Theorem 1.1 we must first compute the ramification data of the extension L/K. Let y be the smallest upper ramification break of L/K which exceeds $\frac{1}{p-1} \cdot e$; if all the upper ramification breaks of L/K are $\le \frac{1}{p-1} \cdot e$, let y be the largest upper ramification break of L/K. By Lemma 2.2(b) we have $y \le (1 + \frac{1}{p-1})e$. Suppose that $y = b_h$, where $b_0 < b_1 < \cdots < b_{n-1}$ are the upper ramification breaks of L/K, and let $z = \psi_{L/K}(y)$ be the corresponding lower break. It follows from Lemma 2.2(c) that for $h \le i < n$ the ith upper ramification break of L/K is $b_i = y + (i-h)e$. Therefore for $h \le i < n$ the ith lower ramification break of L/K is

$$\psi_{L/K}(y + (i-h)e) = z + ep^{h+1} + \cdots + ep^i \tag{5.9}$$

$$= z + ep^{h+1} \cdot \frac{p^{i-h} - 1}{p-1}. \tag{5.10}$$

The largest upper ramification break $u_{L/K} = b_{n-1}$ of L/K is equal to $y + (n-h-1)e$. Since $y \leq (1 + \frac{1}{p-1})e$ this implies $u_{L/K} \leq (n - h + \frac{1}{p-1})e$. It follows that

$$\psi_{L/K}\left(\left(n-h+1+\frac{1}{p-1}\right)e\right) > ep^n. \tag{5.11}$$

Thus if m satisfies $\psi_{L/K}((m+1+\frac{1}{p-1})e) < ep^n$ then $m \leq n-h-1$.

Set $e_0 = es/(p-1)$ and define

$$q = \begin{cases} ((y-e)s + e_0)p^m & \text{if } h = 0 \text{ and } y > e, \\ e_0 p^m & \text{otherwise.} \end{cases} \tag{5.12}$$

Also set $r = q + e_0(p^{m+1} - 1)$. Note that the integers t, q, r and the fields M, E all depend on m.

Theorem 5.2 *Let $p > 3$ and let K be a finite tamely ramified extension of $\mathbb{Q}_p$ with ramification index e. Let L/K and L'/K be totally ramified $(\mathbb{Z}/p^n\mathbb{Z})$-extensions such that L/K is contained in a $\mathbb{Z}_p$-extension L_∞/K. Let $1 \leq a \leq ep^n$ and assume that there are generators σ, σ' for $\mathrm{Gal}(L/K)$, $\mathrm{Gal}(L'/K)$ and uniformizers π_L, $\pi_{L'}$ for L, L' such that $h^{\sigma}_{\pi_L}(X) \equiv h^{\sigma'}_{\pi_{L'}}(X) \pmod{X^a}$. Suppose there exists $1 \leq m \leq n$ such that the following three inequalities are satisfied:*

$$\psi_{M/L}(a) > [M:E]q = p^{n+t-m}q \tag{5.13}$$

$$\psi_{M/L}(a) > \psi_{M/E}(r) \tag{5.14}$$

$$\psi_{M/L}(a) > \psi_{M/K}(u_{L/K}). \tag{5.15}$$

Then there is $\omega \in \mathrm{Gal}(\mathbb{Q}_p^{alg}/\mathbb{Q}_p)$ such that $\omega(K) = K$, ω induces the identity on k, and $[L \cap \omega(L') : K] \geq p^m$.

The following lemmas will be used to compute and bound the ramification breaks of the various extensions used in the proof of Theorem 5.2.

Lemma 5.3 *Let K be a finite extension of $\mathbb{Q}_p$, let L/K be a finite tamely ramified extension with ramification index e, and let M/L be a finite Galois extension which is not tamely ramified. Then the positive lower ramification breaks of M/L are the same as the positive lower ramification breaks of M/K, and the positive upper ramification breaks of M/L are e times the positive upper ramification breaks of M/K.*

Proof: The positive lower ramification breaks of M/K are the values $x > 0$ such that $\phi_{M/K}(x) = \phi_{L/K} \circ \phi_{M/L}(x)$ is not differentiable. It follows from [2, Prop. A.4.2] that for $x > 0$ we have $\phi_{L/K}(x) = e^{-1} \cdot x$. Therefore the positive lower ramification breaks of M/K and M/L are the same. Let $l_0 < l_1 < \cdots < l_{n-1}$ be the positive lower ramification breaks of M/K and M/L. Then the ith positive upper ramification break of M/L is $\phi_{M/L}(l_i)$, and the ith positive upper ramification break of M/K is $\phi_{M/K}(l_i) = \phi_{L/K} \circ \phi_{M/L}(l_i) = e^{-1} \cdot \phi_{M/L}(l_i)$. $\square$

Lemma 5.4 *Let K be a finite extension of $\mathbb{Q}_p$ and let L/K be a finite cyclic extension whose positive upper ramification breaks are $b_0 < b_1 < \cdots < b_{n-1}$. Let E/K be a finite Galois extension and write the ramification index of LE/E in the form up^r with $p \nmid u$. Then the positive upper ramification breaks $\beta_{n-r} < \beta_{n-r+1} < \cdots < \beta_{n-1}$ of LE/E satisfy $\beta_i \le \psi_{E/K}(b_i)$ for $n-r \le i < n$. In particular, $u_{LE/E} \le \psi_{E/K}(u_{L/K})$.*

Proof: We first prove the second statement. Let $m = \psi_{E/K}(u_{L/K})$, and suppose that $m < u_{LE/E}$. Since L/K and LE/E are abelian, $u_{L/K}$ and $u_{LE/E}$ are integers. Therefore m is also an integer. It follows that $m+1 \le u_{LE/E}$, and hence that $\mathrm{Gal}(LE/E)^{m+1}$ is nontrivial. Since the reciprocity map $\omega_{LE/E} : E^\times \to \mathrm{Gal}(LE/E)$ maps $1+\mathcal{P}_E^{m+1}$ onto $\mathrm{Gal}(LE/E)^{m+1}$ (see for instance Corollary 3 to Theorem 2 in [8, XV §2]), there is $\alpha \in 1+\mathcal{P}_E^{m+1}$ such that $\sigma = \omega_{LE/E}(\alpha)$ is not the identity. It follows from the functorial properties of the reciprocity map [8, XI §3] that $\sigma|_L = \omega_{L/K}(\mathrm{N}_{E/K}(\alpha))$. Using Proposition 4.3 we see that $\mathrm{N}_{E/K}(\alpha) \in 1+\mathcal{P}_K^{u_{L/K}+1}$. Since $\omega_{L/K}(1+\mathcal{P}_K^{u_{L/K}+1}) = \mathrm{Gal}(L/K)^{u_{L/K}+1}$ is trivial this implies $\sigma|_L = \mathrm{id}_L$. Since the restriction map $\mathrm{Gal}(LE/E) \to \mathrm{Gal}(L/K)$ is one-to-one, this is a contradiction. Therefore $u_{LE/E} \le \psi_{E/K}(u_{L/K})$.

To prove the first statement, for $0 \le j \le r-1$ let L^j/K be the unique subextension of L/K such that $[L : L^j] = p^j$. The restriction map $\mathrm{Gal}(LE/E) \to \mathrm{Gal}(L/K)$ induces an isomorphism between $\mathrm{Gal}(LE/L)$ and $\mathrm{Gal}(L/(L\cap E))$. Since p^j divides the ramification index of LE/E, we see that $L^j \supset L \cap E$, that L/L^j is totally ramified, and that $\mathrm{Gal}(LE/L^jE)$ is the unique subgroup of $\mathrm{Gal}(LE/E)$ of order p^j. It follows that $u_{L^j/K} = b_{n-j-1}$ and $u_{L^jE/E} = \beta_{n-j-1}$. Applying the second statement we get $\beta_{n-j-1} \le \psi_{E/K}(b_{n-j-1})$ for $0 \le j \le r-1$. □

Proof of Theorem 5.2: Since K, L, and L' all have the same residue field k, there is a unique k-linear ring isomorphism $\mu : \mathcal{O}_{L'}/\mathcal{P}_{L'}^a \to \mathcal{O}_L/\mathcal{P}_L^a$ such that $\mu(\pi_{L'}) \equiv \pi_L \pmod{\mathcal{P}_L^a}$, and a unique $(\mathcal{O}_{L'}/\mathcal{P}_{L'}^a)$-module isomorphism $\eta : \mathcal{P}_{L'}/\mathcal{P}_{L'}^{a+1} \to \mathcal{P}_L/\mathcal{P}_L^{a+1}$ such that $\eta(\pi_{L'}) \equiv \pi_L \pmod{\mathcal{P}_L^{a+1}}$. By combining these isomorphisms we get an isomorphism $i = (1, \mu, \eta)$ from $\mathrm{Tr}_a(L')$ to $\mathrm{Tr}_a(L)$. Since $h^\sigma_{\pi_L}(X) \equiv h^{\sigma'}_{\pi_{L'}}(X) \pmod{X^a}$, we have $i \circ f_{\sigma'} = f_\sigma \circ i$.

Let $b = [M : LF]\cdot a$. Then $(\mathrm{Tr}_b(M), f_{M/L} \circ i)$ is an extension of $\mathrm{Tr}_a(L')$. It follows from Proposition 3.1 that this extension comes from an extension of L'. More precisely, there is a finite extension M'/L' and an isomorphism

$$j = (1, \nu, \theta) : \mathrm{Tr}_b(M') \longrightarrow \mathrm{Tr}_b(M) \tag{5.16}$$

such that $j \circ f_{M'/L'} = f_{M/L} \circ i$. Since $K(\zeta)/\mathbb{Q}_p(\zeta)$ is tamely ramified we have $u_{K(\zeta)/\mathbb{Q}_p} = u_{\mathbb{Q}_p(\zeta)/\mathbb{Q}_p} = m$. Using Lemma 5.3 we see that $u_{K(\zeta)/K} = e \cdot u_{K(\zeta)/\mathbb{Q}_p} = me$. It follows from Lemma 5.4 that $u_{M/L} \le \psi_{L/K}(u_{K(\zeta)/K}) = \psi_{L/K}(me)$. By assumption (5.14) we have

$$\psi_{M/L}(a) > \psi_{M/E}(r) > \psi_{M/E}(e_0(p^m-1)). \tag{5.17}$$

Since $\psi_{E/K}(me) = e_0(p^m-1)$ this implies $\psi_{M/L}(a) > \psi_{M/K}(me)$. Applying $\phi_{M/L}$ to this inequality gives $a > \psi_{L/K}(me) \ge u_{M/L}$. Thus M/L, $\mathrm{Tr}_b(M)/\mathrm{Tr}_a(L)$, $\mathrm{Tr}_b(M')/\mathrm{Tr}_a(L')$, and M'/L' all satisfy condition C^a. It follows from Theorem 3.2 that the field M' is

uniquely determined up to L'-isomorphism. Let $c = \psi_{M/L}(a)$. By Theorem 3.2 the isomorphism j in (5.16) is uniquely determined up to $R(c)$-equivalence.

Lemma 5.5 *Let $\gamma \in \mathrm{Gal}(M/K)$ and let $t \in \mathbb{Z}$ be such that $\gamma|_L = \sigma^t$. Then there is a unique automorphism γ' of M' such that $\gamma'|_{L'} = \sigma'^t$ and $j \circ f_{\gamma'} \equiv f_\gamma \circ j \pmod{R(c)}$. The map $\gamma \mapsto \gamma'$ gives a faithful K-linear action of $\mathrm{Gal}(M/K)$ on M'.*

Proof: For $\gamma \in \mathrm{Gal}(M/K)$ let $f'_\gamma = j^{-1} \circ f_\gamma \circ j$ denote the automorphism of $\mathrm{Tr}_b(M')$ induced by f_γ. Using the identities $j \circ f_{M'/L'} = f_{M/L} \circ i$, $f_\gamma \circ f_{M/L} = f_{M/L} \circ f_{\sigma^t}$, and $f_{\sigma^t} \circ i = i \circ f_{\sigma'^t}$ we find that $f'_\gamma \circ f_{M'/L'} = f_{M'/L'} \circ f_{\sigma'^t}$. Since M'/L' satisfies condition C^a, by Corollary 3.3 there is a unique $\gamma' \in \mathrm{Aut}(M')$ such that $f_{\gamma'} \equiv f'_\gamma \pmod{R(c)}$ and $\gamma'|_{L'} = \sigma'^t$. It follows that $j \circ f_{\gamma'} \equiv f_\gamma \circ j \pmod{R(c)}$. Since γ' is uniquely determined by γ the map $\gamma \mapsto \gamma'$ is a group homomorphism. If γ lies in the kernel of this homomorphism then $\sigma'^t = 1$, and hence $\sigma^t = 1$. Therefore $\gamma \in \mathrm{Gal}(M/L)$ and γ induces the identity on $\mathrm{Tr}_c(M)$. Since M/L satisfies condition C^a this implies $\gamma = 1$. □

It follows from this lemma that M'/K is Galois, and that the map

$$\hat{j} : \mathrm{Gal}(M/K) \longrightarrow \mathrm{Gal}(M'/K) \tag{5.18}$$

defined by $\hat{j}(\gamma) = \gamma'$ is an isomorphism. Furthermore, for all $\gamma \in \mathrm{Gal}(M/K)$ we have

$$f_\gamma \circ j \equiv j \circ f_{\hat{j}(\gamma)} \pmod{R(c)}. \tag{5.19}$$

Since M' is a Galois extension of L' which is uniquely determined up to L'-isomorphism, M' is uniquely determined as a subfield of $\mathbb{Q}_p^{alg}$.

Lemma 5.6 *Let K be a finite extension of $\mathbb{Q}_p$ and let L/K be a $(\mathbb{Z}/p^n\mathbb{Z})$-extension. Then L is contained in a $\mathbb{Z}_p$-extension L_∞ of K if and only if the group μ of p-power roots of unity in K is contained in $\mathrm{N}_{L/K}(L^\times)$.*

Proof: If L is contained in a $\mathbb{Z}_p$-extension L_∞ of K then there is a continuous homomorphism $\chi : K^\times \to \mathrm{Gal}(L_\infty/K)$ such that $\chi(K^\times)$ is dense in $\mathrm{Gal}(L_\infty/K)$ and $\ker(\chi) \leq \mathrm{N}_{L/K}(L^\times)$. It follows that $K^\times/\ker(\chi)$ has trivial torsion, and hence that $\mu \leq \ker(\chi) \leq \mathrm{N}_{L/K}(L^\times)$. If $\mu \leq \mathrm{N}_{L/K}(L^\times)$ then since $\mathrm{N}_{L/K}(L^\times)$ has index p^n in $K^\times$, the group $\tilde{\mu}$ of all roots of unity in K is contained in $\mathrm{N}_{L/K}(L^\times)$. Since $K^\times/\tilde{\mu} \cong \mathbb{Z} \times \mathbb{Z}_p^{[K:\mathbb{Q}]}$ there is a closed subgroup H of $\mathrm{N}_{L/K}(L^\times)$ such that $K^\times/H \cong \mathbb{Z}_p$. Then H corresponds by class field theory to a $\mathbb{Z}_p$-extension L_∞ of K which contains L. □

Since L is contained in a $\mathbb{Z}_p$-extension L_∞ of K, the field $M = LE$ is contained in the $\mathbb{Z}_p$-extension $L_\infty E$ of E. Therefore by Lemma 5.6 there is $\alpha \in \emptyset_M^\times$ such that $\mathrm{N}_{M/E}(\alpha) = \zeta$. Let τ be an element of $\mathrm{Gal}(M/F)$ such that $\tau|_E$ generates the cyclic group $\mathrm{Gal}(E/F)$. Then $\tau|_E$ has order sp^m, and there is $d \in \mathbb{Z}$ such that $\tau(\zeta) = \zeta^d$. It follows that the image of d in $(\mathbb{Z}/p^{m+1}\mathbb{Z})^\times$ has order sp^m. Since $\mathrm{Gal}(M/F)$ is abelian, $\tau(\alpha)/\alpha^d$ lies in the kernel of $\mathrm{N}_{M/E}$. Let ρ be a generator for $\mathrm{Gal}(M/E)$. Then by Hilbert's Theorem 90 there is $\beta \in M^\times$ such that $\tau(\alpha)/\alpha^d = \rho(\beta)/\beta$.

Let π be a uniformizer for M, and write $\beta = \gamma\pi^v$ with $\gamma \in \mathcal{O}_M^\times$ and $v = v_M(\beta)$. Set $\delta = \rho(\gamma)/\gamma$ and $\epsilon = \rho(\pi)/\pi$, so that $\tau(\alpha)/\alpha^d = \delta\epsilon^v$. Now let α', γ', δ', ϵ' be elements of $\mathcal{O}_{M'}^\times$ which correspond via ν to α, γ, δ, ϵ. (In other words, we have $\nu(\alpha') \equiv \alpha \pmod{\mathcal{P}_M^b}$, etc.) In addition, choose $\pi' \in \mathcal{P}_{M'}$ such that $\theta(\pi') \equiv \pi \pmod{\mathcal{P}_M^{b+1}}$, and set $\beta' = \gamma'\pi'^v$. Let $\rho' = \hat{\jmath}(\rho)$ be the element of $\mathrm{Gal}(M'/K)$ which corresponds to $\rho \in \mathrm{Gal}(M/K)$. Since $\rho(\pi) = \epsilon\pi$, it follows from (5.19) that $\rho'(\pi') \equiv \epsilon'\pi' \pmod{\mathcal{P}_{M'}^{c+1}}$, and hence that

$$\epsilon' \equiv \frac{\rho'(\pi')}{\pi'} \pmod{\mathcal{P}_{M'}^c}. \tag{5.20}$$

Furthermore, since $\delta = \rho(\gamma)/\gamma$ and $\delta\epsilon^v = \tau(\alpha)/\alpha^d$ we get

$$\delta' \equiv \frac{\rho'(\gamma')}{\gamma'} \pmod{\mathcal{P}_{M'}^c} \tag{5.21}$$

$$\delta'\epsilon'^v \equiv \frac{\tau'(\alpha')}{\alpha'^d} \pmod{\mathcal{P}_{M'}^c}. \tag{5.22}$$

It follows that

$$\frac{\tau'(\alpha')}{\alpha'^d} \equiv \frac{\rho'(\gamma'\pi'^v)}{\gamma'\pi'^v} \equiv \frac{\rho'(\beta')}{\beta'} \pmod{\mathcal{P}_{M'}^c}. \tag{5.23}$$

Let E' be the subfield of M' fixed by $\langle\rho'\rangle$. Since $M = LE$, it follows from Lemma 5.4 that the upper ramification breaks of M/E are bounded above by $\psi_{E/K}(u_{L/K})$. Hence the lower ramification breaks of M/E are bounded above by $\psi_{M/E} \circ \psi_{E/K}(u_{L/K}) = \psi_{M/K}(u_{L/K})$, which by assumption (5.15) is less than c. It follows that the isomorphism between $\mathrm{Gal}(M/E)$ and $\mathrm{Gal}(M'/E')$ induced by $\hat{\jmath}$ respects ramification filtrations, and hence that $\psi_{M'/E'} = \psi_{M/E}$. Thus by assumption (5.14) we have $c > \psi_{M/E}(r) = \psi_{M'/E'}(r)$. Therefore by (5.23) and Proposition 4.3 we get

$$\mathrm{N}_{M'/E'}\left(\frac{\tau'(\alpha')}{\alpha'^d}\right) \equiv \mathrm{N}_{M'/E'}\left(\frac{\rho'(\beta')}{\beta'}\right) \pmod{\mathcal{P}_{E'}^{r+1}}. \tag{5.24}$$

Let $\zeta' = \mathrm{N}_{M'/E'}(\alpha')$. Since $\mathrm{Gal}(M'/K)$ is abelian and $\rho' \in \mathrm{Gal}(M'/E')$, the congruence (5.24) reduces to

$$\frac{\tau'(\zeta')}{\zeta'^d} \equiv 1 \pmod{\mathcal{P}_{E'}^{r+1}}. \tag{5.25}$$

(Note that if we simply defined ζ' to be an element of $\mathcal{O}_E$ such that $\nu(\zeta') \equiv \zeta \pmod{\mathcal{P}_M^b}$ then by (5.19) and assumption (5.13) we would get the weaker congruence $\tau'(\zeta') \equiv \zeta'^d \pmod{\mathcal{P}_{E'}^{q+1}}$. This explains why we have used such a roundabout method to define ζ'.) By applying Proposition 4.1 to (5.25) with $n = r + 1 > e_0(p^{m+1} + p^m - 1)$ we get $E' = F(\xi)$, with ξ a primitive p^{m+1}th root of 1. Therefore $E' = E$. Furthermore, we have $v_E(\zeta' - \xi) \geq (gs + e_0)p^m$, where

$$g = \begin{cases} \left\lceil \dfrac{1 + (y-e)s}{p^m} \right\rceil & \text{if } h = 0 \text{ and } y > e, \\ 1 & \text{otherwise.} \end{cases} \tag{5.26}$$

Since $(gs+e_0)p^m > q$ we get $\xi \equiv \zeta' \pmod{\mathcal{P}_E^{q+1}}$. By assumption (5.13) we have $b \geq c > p^{n+t-m}q$, and hence

$$\nu(\xi) \equiv \nu(\zeta') \equiv \nu(\mathrm{N}_{M'/E'}(\alpha')) \pmod{\mathcal{P}_M^{p^{n+t-m}q+1}}. \tag{5.27}$$

Therefore by (5.19) we get

$$\nu(\xi) \equiv \mathrm{N}_{M/E}(\alpha) \equiv \zeta \pmod{\mathcal{P}_M^{p^{n+t-m}q+1}}. \tag{5.28}$$

Let L_m/K, L'_m/K be the unique subextensions of L/K, L'/K of degree p^m, and set $M_m = L_mE = L_m(\zeta)$, $M'_m = L'_mE = L'_m(\zeta)$. Then M_m/E, M'_m/E are the unique subextensions of M/E, M'/E of degree p^t. Let $\pi_m = \mathrm{N}_{M/M_m}(\pi)$ and $\pi'_m = \mathrm{N}_{M'/M'_m}(\pi')$. Then π_m, π'_m are uniformizers for M_m, M'_m such that $\theta(\pi'_m) \equiv \pi_m \pmod{\mathcal{P}_M^{c+1}}$. Set $\tilde{q} = \lfloor q/e_0 \rfloor$ and $c_m = e_0p^t\tilde{q}$. By assumption (5.13) we have

$$c > p^{n+t-m}q = [M : M_m]p^tq \geq [M : M_m]c_m. \tag{5.29}$$

Thus there is a unique k-linear ring homomorphism

$$\nu_m : \mathcal{O}_{M'_m}/\mathcal{P}_{M'_m}^{c_m} \longrightarrow \mathcal{O}_{M_m}/\mathcal{P}_{M_m}^{c_m} \tag{5.30}$$

such that $\nu_m(\pi'_m) \equiv \pi_m \pmod{\mathcal{P}_{M_m}^{c_m}}$ and a unique $\mathcal{O}_{M'_m}/\mathcal{P}_{M'_m}^{c_m}$-module homomorphism

$$\theta_m : \mathcal{P}_{M'_m}/\mathcal{P}_{M'_m}^{c_m+1} \longrightarrow \mathcal{P}_{M_m}/\mathcal{P}_{M_m}^{c_m+1} \tag{5.31}$$

such that $\theta_m(\pi'_m) \equiv \pi_m \pmod{\mathcal{P}_{M_m}^{c_m+1}}$. These give an isomorphism $j_m = (1, \nu_m, \theta_m)$ from $\mathrm{Tr}_{c_m}(M'_m)$ to $\mathrm{Tr}_{c_m}(M_m)$.

Let $\omega \in \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$ be such that $\omega(\xi) = \zeta$. Since $\mathbb{Z}_p[\zeta]$ is the ring of integers of $\mathbb{Q}_p(\zeta)$, it follows from (5.28) that

$$j_m \circ f_{M'_m/\mathbb{Q}_p(\zeta)} \equiv f_{M_m/\mathbb{Q}_p(\zeta)} \circ f_\omega \pmod{R(\tilde{q})}. \tag{5.32}$$

Since $u_{L_m/K} = y + (m-h-1)e$ and $u_{K(\zeta)/K} = me$, we have $u_{M_m/K} = y + (m-1)e$ if $h = 0$ and $y > e$, and $u_{M_m/K} = me$ otherwise. Therefore

$$\psi_{E/K}(u_{M_m/K}) = \begin{cases} e_0(p^m-1) + sp^m(y-e) & \text{if } h = 0 \text{ and } y > e, \\ e_0(p^m-1) & \text{otherwise;} \end{cases} \tag{5.33}$$

$$= q - e_0. \tag{5.34}$$

Since $\psi_{M_m/K}(u_{M_m/K})$ and $\psi_{M_m/E}(u_{M_m/E})$ are the largest lower ramification breaks of M_m/K and M_m/E, we have $\psi_{M_m/K}(u_{M_m/K}) \geq \psi_{M_m/E}(u_{M_m/E})$. Applying $\phi_{M_m/E}$ to both sides of this inequality we get $\psi_{E/K}(u_{M_m/K}) \geq u_{M_m/E}$, and hence $q - e_0 \geq u_{M_m/E}$. Since the ramification index e_0 of $E/\mathbb{Q}_p(\zeta)$ is relatively prime to p, it follows from Lemma 5.3 that

$$u_{M_m/\mathbb{Q}_p(\zeta)} = e_0^{-1} \cdot u_{M_m/E} \leq e_0^{-1}(q - e_0) < \tilde{q}. \tag{5.35}$$

Therefore $M_m/\mathbb{Q}_p(\zeta)$ and $M'_m/\mathbb{Q}_p(\zeta)$ satisfy condition $C^{\tilde{q}}$. Hence by applying Corollary 3.3 to (5.32) we see that ω can be extended to an isomorphism $\tilde{\omega} : M'_m \to M_m$ such that

$$j_m \equiv f_{\tilde{\omega}} \pmod{R(d)}, \tag{5.36}$$

where $d = \psi_{M_m/\mathbb{Q}_p(\zeta)}(\tilde{q})$.

For $\gamma_m \in \mathrm{Gal}(M_m/K)$ let γ be a lifting of γ_m to $\mathrm{Gal}(M/K)$ and let $\hat{\jmath}_m(\gamma_m)$ be the restriction of $\hat{\jmath}(\gamma)$ to M'_m. Since $\hat{\jmath}(\mathrm{Gal}(M/M_m)) = \mathrm{Gal}(M'/M'_m)$ we see that $\hat{\jmath}_m(\gamma_m)$ does not depend on the choice of the lifting γ. Thus

$$\hat{\jmath}_m : \mathrm{Gal}(M_m/K) \longrightarrow \mathrm{Gal}(M'_m/K) \tag{5.37}$$

is a well-defined isomorphism. By (5.19) we have

$$f_{\gamma_m} \circ j_m \equiv j_m \circ f_{\hat{\jmath}_m(\gamma_m)} \pmod{R(c_m)}. \tag{5.38}$$

Since $c_m = e_0 p^t \tilde{q} \geq d$, by (5.36) and (5.38) we get

$$f_{\gamma_m} \circ f_{\tilde{\omega}} \equiv f_{\tilde{\omega}} \circ f_{\hat{\jmath}_m(\gamma_m)} \pmod{R(d)} \tag{5.39}$$

$$f_{\gamma_m} \equiv f_{\tilde{\omega} \circ \hat{\jmath}_m(\gamma_m) \circ \tilde{\omega}^{-1}} \pmod{R(d)}. \tag{5.40}$$

Let $N/\mathbb{Q}_p$ be the smallest subextension of $M_m/\mathbb{Q}_p$ such that M_m/N is Galois. Then γ_m and $\tilde{\omega} \circ \hat{\jmath}_m(\gamma_m) \circ \tilde{\omega}^{-1}$ both lie in $\mathrm{Gal}(M_m/N)$. By (5.34) we have $\psi_{E/K}(u_{M_m/K}) < e_0\tilde{q} = \psi_{E/\mathbb{Q}_p(\zeta)}(\tilde{q})$. It follows that the largest lower ramification break $\psi_{M_m/K}(u_{M_m/K})$ of M_m/K is less than $\psi_{M_m/\mathbb{Q}_p(\zeta)}(\tilde{q}) = d$. Since K/N is tamely ramified, by Lemma 5.3 we see that $\psi_{M_m/K}(u_{M_m/K}) < d$ is also the largest lower ramification break of M_m/N. Hence by (5.40) we get $\tilde{\omega} \circ \hat{\jmath}_m(\gamma_m) \circ \tilde{\omega}^{-1} = \gamma_m$ for all $\gamma_m \in \mathrm{Gal}(M_m/K)$. Since

$$\hat{\jmath}_m(\mathrm{Gal}(M_m/K)) = \mathrm{Gal}(M'_m/K) \tag{5.41}$$

$$\hat{\jmath}_m(\mathrm{Gal}(M_m/L_m)) = \mathrm{Gal}(M'_m/L'_m) \tag{5.42}$$

this implies $\tilde{\omega}(K) = K$ and $\tilde{\omega}(L'_m) = L_m$. This proves Theorem 5.2. □

It remains to show that the values $a = ep^n$ and $m = m_0$ specified in Theorem 1.1 satisfy the inequalities in Theorem 5.2. We prove this in the following two lemmas. The first of these lemmas, which is stronger than needed to prove (5.13), will also be used in the proof of Theorem 1.2.

Lemma 5.7 *Let $m \geq 1$ satisfy $\psi_{L/K}((m+1+\frac{1}{p-1})e) < ep^n$. Then $\psi_{M/L}(e(p^n - p^{n-1})) > p^{n+t-m}q$.*

Proof: Let $\tilde{a} = e(p^n - p^{n-1})$ and $\tilde{c} = \psi_{M/L}(\tilde{a})$, and let $\beta_{m-t}, \beta_{m-t+1}, \ldots, \beta_{m-1}$ be the positive upper ramification breaks of M/L. Then we have

$$\tilde{c} = s\beta_{m-t} + sp(\beta_{m-t+1} - \beta_{m-t}) + \cdots + sp^{t-1}(\beta_{m-1} - \beta_{m-2}) + sp^t(\tilde{a} - \beta_{m-1}) \tag{5.43}$$

$$= sp^t\tilde{a} - s(p-1)(\beta_{m-t} + p\beta_{m-t+1} + \cdots + p^{t-1}\beta_{m-1}). \tag{5.44}$$

Since $E/\mathbb{Q}_p(\zeta)$ is tamely ramified, the positive upper ramification breaks of $E/\mathbb{Q}_p$ are the same as the positive upper ramification breaks $1, 2, \ldots, m$ of $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$. It follows by Lemma 5.3 that the positive upper ramification breaks of E/K are $(i+1)e$ for $0 \leq i < m$. Therefore by Lemma 5.4 we have $\beta_i \leq \psi_{L/K}((i+1)e)$ for $m - t \leq i < m$.

The values of $\psi_{L/K}((i+1)e)$ can be computed using the ramification data for L/K given in (5.10):

$$\psi_{L/K}((i+1)e) = \begin{cases} z + ep^{h+1} \cdot \dfrac{p^i - 1}{p-1} + p^{h+i+1}(e-y) & \text{if } y \leq e, \\ z + ep^{h+1} \cdot \dfrac{p^i - 1}{p-1} + p^{h+i}(e-y) & \text{if } y > e. \end{cases} \tag{5.45}$$

It follows from (5.44) that

$$\tilde{c} \geq sp^t\tilde{a} + s(p^t - 1)\left(\frac{ep^{h+1}}{p-1} - z\right) - sp^{m+h-t+1} \cdot \frac{p^{2t}-1}{p+1}\left(\frac{p}{p-1}e - y\right) \tag{5.46}$$

if $y \leq e$, and

$$\tilde{c} \geq sp^m\tilde{a} + s(p^m - 1)\left(\frac{ep^{h+1}}{p-1} - z\right) - sp^h \cdot \frac{p^{2m}-1}{p+1}\left(\frac{2p-1}{p-1}e - y\right) \tag{5.47}$$

if $y > e$. In this last inequality we use the fact that $t = m$ if $y \neq e$.

If $y > e$ then since $z \leq p^h y$ and $p^m - 1 \leq \dfrac{p^{2m}-1}{p+1}$, by (5.47) we get

$$\tilde{c} \geq sp^m\tilde{a} + s(p^m - 1)\left(\frac{ep^{h+1}}{p-1} - p^h y\right) - sp^h \cdot \frac{p^{2m}-1}{p+1}\left(\frac{2p-1}{p-1}e - y\right) \tag{5.48}$$

$$\geq sp^m\tilde{a} + s(p^m - 1)\left(\frac{ep^{h+1}}{p-1} - p^h e\right) - sp^h \cdot \frac{p^{2m}-1}{p+1}\left(\frac{2p-1}{p-1}e - e\right) \tag{5.49}$$

$$= es\left(p^{n+m} - p^{n+m-1} + \frac{p^m - 1}{p-1} \cdot p^h - \frac{p^{2m}-1}{p^2-1} \cdot p^{h+1}\right). \tag{5.50}$$

By (5.11) and the assumption $\psi_{L/K}((m + 1 + \frac{1}{p-1})e) < ep^n$ we have $m + h \leq n - 1$. Therefore $\tilde{c}$ is greater than

$$esp^{n+m}\left(1 - \frac{1}{p} - \frac{1}{p^2-1}\right) = \frac{p^3 - p^2 - 2p + 1}{p^2 + p} \cdot e_0 p^{n+m}. \tag{5.51}$$

Since $q \leq (\frac{es}{p-1} + e_0)p^m = 2e_0p^m$ and $p \geq 5$ we get $\tilde{c} > 2e_0p^{n+m} \geq p^n q$. Since $t = m$ in this case we conclude that $\tilde{c} > p^{n+t-m}q$.

If $y \le e$ then since $h \le n-m-1 \le n-2$ we have $y > e/(p-1)$. It follows by (5.46) that

$$\tilde{c} \ge sp^t\tilde{a} + s(p^t-1)\left(\frac{ep^{h+1}}{p-1} - p^h y\right) - sp^{m+h-t+1}\cdot\frac{p^{2t}-1}{p+1}\left(\frac{p}{p-1}e - y\right) \tag{5.52}$$

$$\ge sp^t\tilde{a} + s(p^t-1)\left(\frac{ep^{h+1}}{p-1} - \frac{p^h e}{p-1}\right) - sp^{m+h-t+1}\cdot\frac{p^{2t}-1}{p+1}\left(\frac{p}{p-1}e - \frac{e}{p-1}\right) \tag{5.53}$$

$$= es\left(p^{n+t} - p^{n+t-1} + (p^t-1)p^h - \frac{p^{2t}-1}{p+1}\cdot p^{m+h-t+1}\right). \tag{5.54}$$

As above this implies that $\tilde{c}$ is greater than or equal to

$$esp^{n+t}\left(1 - \frac{1}{p} - \frac{1}{p+1}\right) = \frac{p^3-2p^2+1}{p^2+p}\cdot e_0 p^{n+t}, \tag{5.55}$$

and hence that $\tilde{c} > e_0 p^{n+t} = p^{n+t-m}q$. □

It follows from Lemma 5.7 that assumption (5.13) is satisfied by $a = ep^n$, $m = m_0$. We now show that these values satisfy assumptions (5.14) and (5.15) as well.

Lemma 5.8 *Let $a, m \ge 1$ satisfy $\frac{2}{p-1}\cdot ep^n < a \le ep^n$ and $\psi_{L/K}((m+1+\frac{1}{p-1})e) < a$. Then $\psi_{M/L}(a) > \psi_{M/E}(r)$ and $\psi_{M/L}(a) > \psi_{M/K}(u_{L/K})$.*

Proof: Since the positive upper ramification breaks of E/K are $(i+1)e$ for $0 \le i < m$, the positive lower ramification breaks of E/K are $\psi_{E/K}((i+1)e) = e_0(p^{i+1}-1)$ for $0 \le i < m$. It follows that

$$\phi_{E/K}(r) = \begin{cases} \left(m+1+\dfrac{1}{p-1}\right)e + (y-e) & \text{if } h = 0 \text{ and } y > e, \\ \left(m+1+\dfrac{1}{p-1}\right)e & \text{otherwise.} \end{cases} \tag{5.56}$$

If $h = 0$ and $y > e$ then

$$\phi_{L/K}(a) = y + (n-1)e + \frac{1}{p^n}\left(a - \left(y + ep\cdot\frac{p^{n-1}-1}{p-1}\right)\right) \tag{5.57}$$

is greater than $\phi_{E/K}(r)$, since $m \le n-1$ and $a > \frac{2}{p-1}\cdot ep^n$. In the other cases the inequality $\phi_{L/K}(a) > \phi_{E/K}(r)$ follows from the assumption $\psi_{L/K}((m+1+\frac{1}{p-1})e) < a$ and (5.56). Applying $\psi_{M/K}$ to both sides of this inequality we get $\psi_{M/L}(a) > \psi_{M/E}(r)$. By (5.10) we have

$$\psi_{L/K}(u_{L/K}) = z + ep^{h+1}\cdot\frac{p^{n-h-1}-1}{p-1}. \tag{5.58}$$

Since $z \le p^h y \le ep^{h+1}/(p-1)$, this quantity is less than a. It follows that $\psi_{M/K}(u_{L/K}) < \psi_{M/L}(a)$. □

Theorem 1.1 follows from Theorem 5.2 combined with Lemmas 5.7 and 5.8. To prove Theorem 1.2 we apply Theorem 5.2 to the subextensions of L/K and L'/K of degree p^{n-1}:

Proof of Theorem 1.2: Let L/K, L'/K be totally ramified $(\mathbb{Z}/p^n\mathbb{Z})$-extensions which satisfy condition (*) of Theorem 1.1. We may assume without loss of generality that K contains a primitive pth root of unity, that $m_0 \geq 2$, and that $n \geq 3$. Since $p \nmid e$ we see that K contains no primitive p^2th roots of unity. Therefore the group μ of p-power roots of unity of K is cyclic of order p. Let L_{n-1}/K be the unique subextension of L/K of degree p^{n-1}. Then $\mathrm{N}_{L/K}(L^\times)$ has index p in $\mathrm{N}_{L_{n-1}/K}(L_{n-1}^\times)$, so $\mu \leq \mathrm{N}_{L_{n-1}/K}(L_{n-1}^\times)$. Hence by Lemma 5.6 we see that L_{n-1} is contained in a $\mathbb{Z}_p$-extension L_∞ of K. Let $j = \psi_{L/K}(u_{L/K})$ be the unique ramification break of L/L_{n-1} and let $l = \lceil \frac{p-1}{p} \cdot j \rceil$. Then by (5.10) we have

$$l = \left\lceil \frac{p-1}{p} \cdot \left(z + ep^{h+1} \cdot \frac{p^{n-h-1}-1}{p-1} \right) \right\rceil. \tag{5.59}$$

It follows from [11, Prop. 2.2.1] that the norm map induces ring isomorphisms

$$\overline{\mathrm{N}}_{L/L_{n-1}} : \emptyset_L/(\mathcal{P}_L^l) \longrightarrow \emptyset_{L_{n-1}}/(\mathcal{P}_{L_{n-1}}^l) \tag{5.60}$$

$$\overline{\mathrm{N}}_{L'/L'_{n-1}} : \emptyset_L/(\mathcal{P}_{L'}^l) \longrightarrow \emptyset_{L'_{n-1}}/(\mathcal{P}_{L'_{n-1}}^l). \tag{5.61}$$

These isomorphisms are Galois-equivariant and induce the p-Frobenius map on k.

Let σ_{n-1} denote the restriction of σ to L_{n-1}, set $\pi_{L_{n-1}} = \mathrm{N}_{L/L_{n-1}}(\pi_L)$, and set $\pi_{L'_{n-1}} = \mathrm{N}_{L'/L'_{n-1}}(\pi_{L'})$. By applying the arguments used to prove (2.3) to (5.60) and (5.61) we get

$$h_{\pi_{L_{n-1}}}^{\sigma_{n-1}}(X) \equiv (h_{\pi_L}^{\sigma})^{\phi}(X) \pmod{X^l} \tag{5.62}$$

$$h_{\pi_{L'_{n-1}}}^{\sigma'_{n-1}}(X) \equiv (h_{\pi_{L'}}^{\sigma'})^{\phi}(X) \pmod{X^l}. \tag{5.63}$$

Since $h_{\pi_L}^{\sigma} = h_{\pi_{L'}}^{\sigma'}$ this implies

$$h_{\pi_{L_{n-1}}}^{\sigma_{n-1}}(X) \equiv h_{\pi_{L'_{n-1}}}^{\sigma'_{n-1}}(X) \pmod{X^l}. \tag{5.64}$$

Since $m_0 \geq 2$ we have $h \leq n-3$, so y is the smallest upper ramification break of L_{n-1}/K which exceeds $\frac{1}{p-1} \cdot e$. Therefore the largest upper ramification break of L_{n-1}/K is $u_{L_{n-1}/K} = y + (n-h-2)e$. Let $m = m_0 - 1$ and define E/F as in the proof of Theorem 5.2. Also set $M_{n-1} = L_{n-1}E$. To prove Theorem 1.2 it suffices by Theorem 5.2 to prove the following inequalities:

$$\psi_{M_{n-1}/L_{n-1}}(l) > [M_{n-1} : E]q \tag{5.65}$$

$$\psi_{M_{n-1}/L_{n-1}}(l) > \psi_{M_{n-1}/E}(r) \tag{5.66}$$

$$\psi_{M_{n-1}/L_{n-1}}(l) > \psi_{M_{n-1}/K}(u_{L_{n-1}/K}). \tag{5.67}$$

Using (5.10) to compute the left side of the inequality $\psi_{L/K}((m_0+1+\frac{1}{p-1})e) < ep^n$ we get

$$z + ep^{h+1} \cdot \frac{p^{m_0}-1}{p-1} + p^{m_0+h+1}\left(\frac{p}{p-1}\cdot e - y\right) < ep^n. \tag{5.68}$$

Since $z \le p^h y \le ep^{h+1}/(p-1)$ we have $(p-1)z - ep^{h+1} \le 0$. Adding this inequality to (5.68) and dividing by p gives

$$z + ep^{h+1} \cdot \frac{p^{m_0-1}-1}{p-1} + p^{m_0+h}\left(\frac{p}{p-1}\cdot e - y\right) < ep^{n-1}. \tag{5.69}$$

Hence we have

$$\psi_{L_{n-1}/K}\left(\left(m+1+\frac{1}{p-1}\right)e\right) = \psi_{L_{n-1}/K}\left(\left(m_0+\frac{1}{p-1}\right)e\right) < ep^{n-1}. \tag{5.70}$$

It follows from (5.59) that $l > e(p^{n-1}-p^{n-2})$. Therefore (5.65) follows from Lemma 5.7. By (5.10) we have

$$\psi_{L_{n-1}/K}(u_{L_{n-1}/K}) = z + ep^{h+1}\cdot\frac{p^{n-h-2}-1}{p-1}. \tag{5.71}$$

Using (5.59) and the inequality $z \le ep^{h+1}/(p-1)$ we deduce that $\psi_{L_{n-1}/K}(u_{L_{n-1}/K}) < l$. Applying $\psi_{M_{n-1}/L_{n-1}}$ to this last inequality gives (5.67).

It remains to prove (5.66). If $h=0$ and $y > e$ then by (5.59) we have $l > (p^{n-1}-1)e$. It follows using (5.10) that

$$\phi_{L_{n-1}/K}(l) > \left(n-1-\frac{1}{p-1}+\frac{1}{p^n-p^{n-1}}\right)e + \left(1-\frac{1}{p^{n-1}}\right)y. \tag{5.72}$$

By (5.56) with $m = m_0 - 1$ we have

$$\phi_{E/K}(r) = \left(m_0+\frac{1}{p-1}\right)e + (y-e). \tag{5.73}$$

Since $m_0 \le n-1$, $y \le (1+\frac{1}{p-1})e$, $p \ge 5$, and $n \ge 2$, we get $\phi_{E/K}(r) < \phi_{L_{n-1}/K}(l)$. Applying $\psi_{M_{n-1}/K}$ to this inequality gives (5.66) in this case.

Suppose $h \ge 1$ or $y \le e$. Adding

$$(p-1)z - ep^{h+1} \le p\left\lceil\frac{p-1}{p}\cdot z\right\rceil - ep^{h+1}. \tag{5.74}$$

to (5.68) and dividing by p gives

$$z + ep^{h+1}\cdot\frac{p^{m_0-1}-1}{p-1} + p^{m_0+h}\left(\frac{p}{p-1}\cdot e - y\right) < \left\lceil\frac{p-1}{p}\cdot z\right\rceil + ep^{n-1} - ep^h. \tag{5.75}$$

It follows from (5.56), (5.10), and (5.59) that this inequality can be rewritten as $\psi_{L_{n-1}/K}\circ\phi_{E/K}(r) < l$. By applying $\psi_{M_{n-1}/L_{n-1}}$ we get (5.66). □

6 p-adic dynamical systems

Let K be a finite extension of $\mathbb{Q}_p$ and let $\mathcal{P}^{alg}$ be the maximal ideal in the ring of integers of $\mathbb{Q}_p^{alg}$. Let $u(X) \in \mathcal{O}_K[[X]]$ be a power series such that $u(0) = 0$ and $u'(0)$ is a 1-unit. We are interested in studying the periodic points of $u(X)$. These are the elements $\alpha \in \mathcal{P}^{alg}$ such that $u^{\circ m}(\alpha) = \alpha$ for some $m \geq 1$; the smallest such m is called the period of α. Since $u'(0)$ is a 1-unit, it follows from [4, Cor. 2.3.2] that all periodic points of $u(X)$ have period p^n for some $n \geq 0$. In the introduction to [5], Lubin stated that the extension fields generated by the periodic points of $u(X)$ are "almost completely unknown". In this section we show how Theorem 5.2 can be used to study the extension $K(\alpha)/K$ generated by a single periodic point α.

Let $\overline{u}(X) \in k[[X]]$ denote the reduction of $u(X)$ modulo $\mathcal{P}_K$. It follows from our assumptions that $\overline{u}(X)$ is an element of the group $\mathcal{A}(k)$ which was defined in Section 2. For $n \geq 0$ let i_n denote the depth of $\overline{u}^{\circ p^n}(X)$. If $i_n < \infty$ then $i_n + 1$ is equal to the number of solutions in $\mathcal{P}$ to the equation $u^{\circ p^n}(X) = X$, counted with multiplicity. Let Γ be the closed subgroup of $\mathcal{A}(k)$ generated by $\overline{u}(X)$ and assume that Γ is infinite; then $\Gamma \cong \mathbb{Z}_p$. It follows from Proposition 2.1 that there is a local field L_0 with residue field k, a totally ramified $\mathbb{Z}_p$-extension L_∞/L_0, and a compatible sequence of uniformizers (π_n) for L_∞/L_0 such that $\Gamma = \Gamma_{L_\infty/L_0}^{(\pi_n)}$. The extension L_∞/L_0 is determined uniquely up to k-isomorphism by Γ. By [11, Cor. 3.3.4] the ramification data of the extension L_∞/L_0 is the same as the ramification data of Γ. We define the index d of Γ to be the absolute ramification index of L_0; if L_0 has characteristic p then the index of Γ is ∞. If $d < \infty$ then it follows from Lemma 2.2 that $b_n - b_{n-1} = d$ for all sufficiently large n.

Theorem 6.1 *Let $p > 3$, let $1 \leq d \leq p-2$, and let $K/\mathbb{Q}_p$ be a finite extension with ramification index $e \leq p-1$. Then there is a finite tamely ramified extension E/K with the following property: Let $u(X) \in \mathcal{O}_K[[X]]$ be a power series such that the closed subgroup Γ of $\mathcal{A}(k)$ generated by $\overline{u}(X)$ is isomorphic to $\mathbb{Z}_p$ and has index d. Let L_0 be a local field with residue field k and let L_∞/L_0 be a totally ramified $\mathbb{Z}_p$-extension such that $\Gamma \in [\Gamma_{L_\infty/L_0}]$. For $n \geq 1$ let L_n/L_0 denote the subextension of L_∞/L_0 of degree p^n. Then for each periodic point α of $u(X)$ with period p^n there is an embedding $\omega : L_n \to \mathbb{Q}_p^{alg}$ such that*

$$[E(\alpha) \cap (E \cdot \omega(L_n)) : E] \geq p^{n-2}. \tag{6.1}$$

Thus when the hypotheses of Theorem 6.1 are satisfied the special fiber $\overline{u}(X)$ of $u(X)$ carries a large amount of information about the field extensions generated by periodic points of $u(X)$. It follows from Lemma 2.2 that if the index of Γ is ∞ then the upper ramification breaks of Γ satisfy $b_n \geq pb_{n-1}$ for all $n \geq 1$, while if the index of Γ is $d < \infty$ then for each $n \geq 1$ we have either $b_n \geq pb_{n-1}$ or $b_n - b_{n-1} = d$. Therefore the index of Γ can be effectively computed as long as it is finite.

The rest of this section is devoted to proving Theorem 6.1. Let l be the field extension of k of degree $d!$ and let F be the unramified extension of $\mathbb{Q}_p$ with residue field l. The field E is defined to be the compositum of all totally ramified extensions R/F of degree $d!e$. The following lemma is a consequence of the well-known properties of tamely ramified extensions of a local field.

Lemma 6.2 *(a) The absolute ramification index of E is $d!e$.*
(b) If M is a finite extension of $\mathbb{Q}_p$ whose absolute ramification index divides $d!e$ and whose residue field is contained in l, then M is contained in E.

It follows from this lemma that E is an extension of K with ramification index $d!$, and hence that E/K is tamely ramified. In particular, if $d = 1$ then E/K is unramified.

Before proving Theorem 6.1 we study the basic properties of periodic points of power series which satisfy the hypotheses of the theorem. In particular, we are interested in the degrees and ramification indices of extensions generated by these periodic points. For the remainder of this section we assume without loss of generality that $n \geq 3$.

As above we let $(i_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ denote the lower and upper ramification sequences of Γ. By Lemma 2.2(a) we have $b_0 \leq (1 + \frac{1}{p-1})d$. Since $d < p - 1$ this implies $i_0 = b_0 \leq d$. We also have $b_0 \geq 1 > d/(p-1)$. Therefore by Lemma 2.2(c) we get $b_n = b_{n-1} + d$ and hence $i_n = i_{n-1} + dp^n$ for all $n \geq 1$. We may write $u(X) = a_0X + a_1X^2 + a_2X^3 + \cdots$ with $a_i \in \mathcal{O}_K$ and a_0 a 1-unit. Since $p > e/(p-1)$ we have

$$v_K(a_0^{p^n} - 1) = v_K(a_0^{p^{n-1}} - 1) + e \tag{6.2}$$

if $a_0^p \neq 1$. It follows from [4, Cor. 2.3.1] that $u^{\circ p^{n-1}}(X) - X$ divides $u^{\circ p^n}(X) - X$ in $\mathcal{O}_K[[X]]$. Let

$$q_n(X) = \frac{u^{\circ p^n}(X) - X}{u^{\circ p^{n-1}}(X) - X}. \tag{6.3}$$

If $a_0^p \neq 1$ then by (6.2) the constant term of $q_n(X)$ has p-valuation 1, while if $a_0^p = 1$ then the constant term of $q_n(X)$ is equal to p. Note that the Weierstrass degree of $q_n(X) \in \mathcal{O}_K[[X]]$ is $i_n - i_{n-1} = dp^n$.

Let $\alpha \in \mathcal{P}$ be a periodic point of $u(X)$ with period p^n and let M/K be the Galois closure of $K(\alpha)/K$. Let $G = \mathrm{Gal}(M/K)$, let

$$H = \{\tau \in G : \tau(\alpha) = u^{\circ i}(\alpha) \text{ for some } i \in \mathbb{Z}\}, \tag{6.4}$$

and let $\sigma_1, \ldots, \sigma_h$ be coset representatives for G/H. The polynomial

$$f(X) = \prod_{j=1}^{h} \prod_{i=0}^{p^n-1} (X - u^{\circ i}(\sigma_j(\alpha))) \tag{6.5}$$

lies in $\mathcal{O}_K[X]$ and has distinct roots, all of which are zeros of $q_n(X)$. Therefore $f(X)$ divides $q_n(X)$ in $\mathcal{O}_K[[X]]$, and hence the constant term c of $f(X)$ is an element of $\mathcal{P}_K$ which divides p. It follows that c has p-valuation s/e for some $1 \leq s \leq e$. Since each of the hp^n roots of $f(X)$ has the same p-valuation as α, we get $v_p(\alpha) = s/ehp^n$.

For each $1 \leq j \leq h$ the set $B_j = \{u^{\circ i}(\sigma_j(\alpha)) : 0 \leq i < p^n\}$ is a block for the permutation representation of G acting on the roots of $f(X)$. Let N be the kernel of the action of G on the set of blocks, let T be the fixed field of N, and let U/K be the maximum unramified subextension of T/K. Since the degree of $f(X)$ is less than or equal to the Weierstrass degree of $q_n(X)$ we have $h \leq d$. Since $\mathrm{Gal}(T/K) \cong G/N$ is

isomorphic to a subgroup of S_h this implies that $[T : U]$ and $[U : K]$ both divide $d!$. Therefore T is an extension of $\mathbb{Q}_p$ whose absolute ramification index divides $d!e$ and whose residue field is contained in l. Hence by Lemma 6.2(b), T is contained in E.

For each $\tau \in N = \mathrm{Gal}(M/T)$ there is a unique $i \in \mathbb{Z}/p^n\mathbb{Z}$ such that $\tau(\alpha) = u^{\circ i}(\alpha)$. Hence $T(\alpha)/T$ is Galois, and $\mathrm{Gal}(T(\alpha)/T)$ can be identified with a subgroup of $\mathbb{Z}/p^n\mathbb{Z}$. It follows that $E(\alpha)/E$ is also Galois, with $\mathrm{Gal}(E(\alpha)/E)$ isomorphic to a subgroup of $\mathrm{Gal}(T(\alpha)/T)$. Since the ramification index of $E/\mathbb{Q}_p$ is $d!e$, the E-valuation of α is t/p^n, where $t = (d!/h) \cdot s$ is relatively prime to p. It follows that $[E(\alpha) : E] \geq p^n$, and hence that $\mathrm{Gal}(E(\alpha)/E) \cong \mathbb{Z}/p^n\mathbb{Z}$.

Since the absolute ramification index of T divides $d!e$ and the residue field of T is contained in l, there is a totally ramified extension R/F of degree $d!e$ such that R contains T. Then $E(\alpha)$ is an unramified extension of $R(\alpha)$, so the $R(\alpha)$-valuation of α is t. Therefore we can write $\alpha = \zeta\pi^t$, where $\zeta \in F$ is a root of unity whose order is prime to p and π is a uniformizer for $R(\alpha)$. Let $K(l) = FK$ be the unramified extension of K with residue field l and let $\tau \in \mathrm{Gal}(E(\alpha)/E)$ satisfy $\tau(\alpha) = u(\alpha)$. Let $v(X)$ be the unique element of $\emptyset_{K(l)}[[X]]$ such that $\zeta v(X)^t = u(\zeta X^t)$ and $v'(0) \equiv 1 \pmod{\mathcal{P}_{K(l)}}$. Then

$$\zeta v(\pi)^t = u(\zeta\pi^t) = u(\alpha) = \tau(\alpha) = \zeta\tau(\pi)^t. \tag{6.6}$$

Since τ has order p^n this implies $\tau(\pi) = v(\pi)$. We are now in a position to prove the following key fact:

Proposition 6.3 *The absolute ramification index $d!e$ of E is equal to td.*

Proof: Let $\Gamma' \cong \mathbb{Z}_p$ be the closed subgroup of $\mathcal{A}(l)$ generated by $\overline{v}(X)$. Since $E(\alpha) = E(\pi)$ and $\tau(\pi) = v(\pi)$, the lower ramification breaks of the extension $E(\alpha)/E$ which are less than $d!p^n$ (the ramification index of $E(\alpha)/K(l)$) are the same as the lower ramification breaks of Γ' which are less than $d!p^n$. It follows from the definition of $v(X)$ that the ramification breaks of Γ' are t times the ramification breaks of Γ. Therefore the first two lower ramification breaks of Γ' are ti_0 and $ti_1 = ti_0 + tdp$. Using the inequalities $s \leq p-1$ and $i_0 \leq d \leq p-2$ we deduce that $ti_0 + tdp < d!p^3$. Therefore the first two lower ramification breaks of $E(\alpha)/E$ are ti_0 and $ti_0 + tdp$, and hence the first two upper ramification breaks of $E(\alpha)/E$ are ti_0 and $ti_0 + td$. Since $ti_0 + td < p \cdot ti_0$, it follows from Lemma 2.2 that the absolute ramification index of E is td. □

Corollary 6.4 *For $n \geq 3$ the periodic points of $u(X)$ with period p^n all have p-valuation $1/dp^n$.*

Proof: Let α be a periodic point of $u(X)$ with period p^n. We saw above that $v_p(\alpha) = s/ehp^n$. Since $s = ht/d!$ and $t = d!e/d$ we get $v_p(\alpha) = 1/dp^n$. □

Proposition 6.5 *Let $n \geq 3$. Then every zero of $q_n(X)$ is periodic with period p^n.*

Proof: Let α be a periodic point with period p^j for some $0 \leq j < n$. If $j = 0$ then α is a zero of $u(X) - X$, and if $j \geq 1$ then α is a zero of $q_j(X)$. It follows by the Weierstrass

preparation theorem that α is a root of a distinguished polynomial with coefficients in $\mathcal{O}_K$ which divides $u(X)$ or $q_j(X)$. Since $u(X)$ has Weierstrass degree i_0+1, and $q_j(X)$ has Weierstrass degree dp^j, we must have

$$v_p(\alpha) \geq \begin{cases} \dfrac{1}{e(i_0+1)} & \text{if } j=0, \\ \dfrac{1}{edp^j} & \text{if } 1 \leq j < n. \end{cases} \tag{6.7}$$

In particular, since $n \geq 3$, $e < p$, and $i_0 \leq d$ we have $v_p(\alpha) > 1/dp^n$.

The series $q_n(X)$ has dp^n zeros, counting multiplicities; all of these are periodic points with period p^j for some $0 \leq j \leq n$. Let $\alpha \in \mathcal{P}^{alg}$ be a zero of $q_n(X)$. If α is a periodic point with period p^n then by Corollary 6.4 we have $v_p(\alpha) = 1/dp^n$. On the other hand, if α is a periodic point with period p^j for some $0 \leq j < n$, then $v_p(\alpha) > 1/dp^n$. The sum of the p-valuations of the dp^n zeros of $q_n(X)$ is 1. Therefore all the zeros of $q_n(X)$ must have period p^n. $\square$

It follows that for $n \geq 3$ the periodic points of $u(X)$ with period p^n are precisely the zeros of $q_n(X)$, and that the number of periodic points of $u(X)$ of period p^n, counted with multiplicity, is equal to the Weierstrass degree $i_n - i_{n-1} = dp^n$ of $q_n(X)$. In particular, $u(X)$ has periodic points of period p^n for every $n \geq 3$.

Proof of Theorem 6.1: Since $\Gamma \in [\Gamma_{L_\infty/L_0}]$, there exists a compatible sequence of uniformizers (π_j) for L_∞/L_0 such that $\Gamma = \Gamma^{(\pi_j)}_{L_\infty/L_0}$. Since $\overline{u}(X)$ generates Γ, it follows from (2.4) that there is a generator σ for $\mathrm{Gal}(L_\infty/L_0)$ such that

$$\sigma(\pi_j) \equiv \overline{u}^{\phi^{-j}}(\pi_j) \pmod{\mathcal{P}_{L_j}^{r_j+1}} \tag{6.8}$$

for all $j \geq 1$, where $r_j = \lceil (p-1)i_j/p \rceil$, and we identify k with a subring of $\mathcal{O}_{L_j}/(\pi_j^{r_j+1})$ using the Teichmüller lifting.

The map $x \mapsto x^p$ is an automorphism of the group of roots of unity of F. We denote the inverse of this automorphism by raising to the power p^{-1}. For $1 \leq j \leq \infty$ let $E_j = EL_j$.

Lemma 6.6 *There exists a compatible sequence of uniformizers $(\tilde{\pi}_j)$ for E_∞/E such that $\pi_j = \zeta^{p^{-j}}\tilde{\pi}_j^t$ for $0 \leq j < \infty$.*

Proof: Let $j \geq 0$ and let $\tilde{\pi}_j \in \mathbb{Q}_p^{alg}$ be a root of $X^t - \zeta^{-p^{-j}}\pi_j$. Let k_E denote the residue field of E and let E'_j be the unramified extension of $FL_j(\tilde{\pi}_j)$ with residue field k_E. Since $\zeta^{-p^{-j}}\pi_j$ is a uniformizer for FL_j, the extension of $FL_j(\tilde{\pi}_j)/FL_j$ is totally ramified, with ramification index t. Therefore the maximum tame subextension $T_j/\mathbb{Q}_p$ of $FL_j(\tilde{\pi}_j)/\mathbb{Q}_p$ has ramification index $td = d!e$ and residue field l. It follows by Lemma 6.2(b) that T_j is contained in E. Thus by Lemma 6.2(a), E is an unramified extension of T_j, so E is contained in E'_j. Since $L_j \subset E'_j$, we get $E'_j = EL_j = E_j$. The norm map $\mathrm{N}_{E_j/E}$ gives a bijection between the roots of $X^t - \zeta^{-p^{-j}}\pi_j$ and the roots of $X^t - \zeta^{-1}\pi_0$. Therefore we

may assume that $\mathrm{N}_{E_j/E}(\tilde{\pi}_j) = \tilde{\pi}_0$ for every $j \geq 1$. It follows from this assumption that $(\tilde{\pi}_j)_{j\geq 0}$ is a compatible sequence of uniformizers for E_∞/E. $\square$

Since $\zeta v(X)^t = u(\zeta X^t)$ we have $\overline{\zeta}\overline{v}(X)^t = \overline{u}(\overline{\zeta}X^t)$, where $\overline{\zeta}$ denotes the image of ζ in $l \cong \mathcal{O}_{K(l)}/\mathcal{P}_{K(l)}$. Applying ϕ^{-n} we get $\overline{\zeta}^{p^{-n}}\overline{v}^{\phi^{-n}}(X)^t = \overline{u}^{\phi^{-n}}(\overline{\zeta}^{p^{-n}}X^t)$. Let $\tilde{\sigma}$ be the generator for $\mathrm{Gal}(E_\infty/E)$ whose restriction to L_∞ is σ. Then by (6.8) and Lemma 6.6 we have

$$\tilde{\sigma}(\zeta^{p^{-n}}\tilde{\pi}_n^t) \equiv \overline{u}^{\phi^{-n}}(\zeta^{p^{-n}}\tilde{\pi}_n^t) \pmod{\mathcal{P}_{E_n}^{t(r_n+1)}} \tag{6.9}$$

$$\zeta^{p^{-n}}\tilde{\sigma}(\tilde{\pi}_n)^t \equiv \zeta^{p^{-n}}\overline{v}^{\phi^{-n}}(\tilde{\pi}_n)^t \pmod{\mathcal{P}_{E_n}^{t(r_n+1)}} \tag{6.10}$$

$$\tilde{\sigma}(\tilde{\pi}_n) \equiv \overline{v}^{\phi^{-n}}(\tilde{\pi}_n) \pmod{\mathcal{P}_{E_n}^{tr_n+1}}. \tag{6.11}$$

Let Φ be an automorphism of $\mathbb{Q}_p^{alg}$ which induces the p-Frobenius on residue fields, and let $\Theta : E_\infty \to \Phi^n(E_\infty)$ be the isomorphism induced by Φ^n. Applying Θ to (6.11) we get

$$\hat{\sigma}(\hat{\pi}_n) \equiv \overline{v}(\hat{\pi}_n) \pmod{\mathcal{P}_{\Theta(E_n)}^{tr_n+1}}, \tag{6.12}$$

where $\hat{\pi}_n = \Theta(\tilde{\pi}_n)$ is a uniformizer for $\Theta(E_n)$ and $\hat{\sigma} = \Theta \circ \tilde{\sigma} \circ \Theta^{-1}$ is a generator for $\mathrm{Gal}(\Theta(E_\infty)/E)$. (Note that since E is Galois over $\mathbb{Q}_p$ we have $\Theta(E) = E$.) On the other hand, since $\tau(\pi) = v(\pi)$ we have

$$\tau(\pi) \equiv \overline{v}(\pi) \pmod{\mathcal{P}_E^{tr_n+1}}. \tag{6.13}$$

Note that since π is a uniformizer for $R(\alpha)$, π is also a uniformizer for E. To complete the proof of Theorem 6.1 we will apply Theorem 5.2 to the extensions $\Theta(E_n)/E$ and $E(\alpha)/E$. To do this we must first compute some ramification data.

Since $d < p-1$, it follows from Lemma 2.2(b) that the jth upper ramification break of L_∞/L_0 is $b_j = b_0 + jd$. Therefore the lower breaks of L_∞/L_0 are given by $i_j = i_0 + dp + dp^2 + \cdots + dp^j$, with $i_0 = b_0$. The unique ramification break of L_{n+1}/L_n is equal to the nth lower ramification break i_n of L_∞/L_0. It follows that

$$r_n = \left\lceil \frac{p-1}{p} \cdot (i_0 + dp + dp^2 + \cdots + dp^n) \right\rceil \tag{6.14}$$

$$> d(p^n - 1). \tag{6.15}$$

The ramification breaks of E_n/E are t times the ramification breaks of L_n/L_0. The upper and lower ramification breaks of L_n/L_0 are the integers b_j and i_j for $0 \leq j < n$ which were computed in the preceding paragraph. Therefore we have

$$\psi_{E_n/E}\left(\left(n - 1 + \frac{1}{p-1}\right)td\right) = \frac{p^n + p^{n-1} - p}{p-1} \cdot td - (p^{n-1} - 1)ti_0. \tag{6.16}$$

This value is less than $td(p^n - p^{n-1})$, which by (6.15) is less than tr_n. Comparing (6.12) with (6.13) and applying Lemmas 5.7 and 5.8 we see that the extensions $\Theta(E_n)/E$ and $E(\alpha)/E$ satisfy the hypotheses of Theorem 5.2, with $a = tr_n$ and $m = n-2$. Therefore there is an automorphism Ψ of $\mathbb{Q}_p^{alg}$ such that

$$[E(\alpha) \cap \Psi(\Theta(E_n)) : E] \geq p^{n-2}. \tag{6.17}$$

Since $E_n = EL_n$ and $\Psi(\Theta(E)) = E$, this proves Theorem 6.1. $\square$

References

[1] R. Camina, The Nottingham group, in *New Horizons in pro-p Groups*, pp. 205–221, Progr. Math. **184**, Birkhäuser Boston, 2000.

[2] P. Deligne, Les corps locaux de caractéristique p, limites de corps locaux de caractéristique 0, in *Representations of Reductive Groups over a Local Field*, 119–157, Travaux en Cours, Hermann, Paris, 1984.

[3] F. Laubie, A. Movahhedi, A. Salinier, Systèmes dynamiques non archimédiens et corps des normes, Compositio Math. **132** (2002), 57–98.

[4] H.-C. Li, p-adic periodic points and Sen's theorem, J. Number Theory **56** (1996), 309–318.

[5] J. Lubin, Non-Archimedean dynamical systems, Compositio Math. **94** (1994), 321–346.

[6] M. Marshall, Ramification groups of abelian local field extensions, Canad. J. Math. **23** (1971) 271–281.

[7] S. Sen, On automorphisms of local fields, Ann. of Math. (2) **90** (1969), 33–46.

[8] J.-P. Serre, *Local Fields*, Springer, New York, 1979.

[9] J.-P. Wintenberger, Automorphismes des corps locaux de charactéristique p, preprint.

[10] J.-P. Wintenberger, Extensions abéliennes et groupes d'automorphismes de corps locaux, C. R. Acad. Sci. Paris Sér. A-B **290** (1980), A201–A203.

[11] J.-P. Wintenberger, Le corps des normes de certaines extensions infinies de corps locaux; applications, Ann. Sci. École Norm. Sup. (4) **16** (1983), 59–89.